

RIASSUNTO SLIDE PER ORALE SISTEMI INFORMATIVI – Capitoli 1,2,7,8,9

Argomenti più richiesti all'esame

- BPM con collegamento BPI e BPR (capitolo 1)
- ITIL (Capitolo 1)
- Variabili organizzative di Bracchi (Capitolo 1)
- Classificazione dei processi, Anthony e Porter (Capitolo 1)
- Sistemi integrati (ERP, CRM, SCM) (Capitolo 2)
- Business Intelligence (Capitolo 6)
- Google (capitolo 7)
- Governo d'impresa e management: COBIT (Capitolo 8)
- Profili professionali IT (Capitolo 8)
- Obiettivi sicurezza informatica, modelli ISO (Capitolo 9)
- RTO, RPO (Capitolo 9)

Capitolo 1 – Ingegneria dei processi aziendali

L'**azienda** può essere: rivolta al profitto, il cui obiettivo è massimizzare il *guadagno* (multinazionali, società, professionisti, aziende individuali), un'*organizzazione no profit* che cerca di pareggiare *spese e fatturato*, oppure un *ente pubblico*.

La **missione (o scopo)** di un'organizzazione è il suo scopo ultimo, la giustificazione stessa della sua esistenza ed al tempo stesso ciò che la contraddistingue da tutte le altre. Il **mission statement** è il “manifesto” della missione, che tende a focalizzarsi sul presente e a fornire una guida operativa. In alcuni casi si riduce ad uno **slogan** mentre in altri è più esaustivo.

Il termine **visione** indica la proiezione di uno scenario futuro che rispecchia gli ideali, i valori e le aspirazioni; forma l'insieme degli obiettivi di lungo periodo che la dirigenza vuole definire per la propria azienda. (Esempi di mission: Google - organizzare l'informazione mondiale e renderla universalmente accessibile, Microsoft – Empowering others)

Il **core business** di un'azienda è la principale attività aziendale di tipo operativo, ne determina il compito fondamentale preposto ai fini di creare un *fatturato* ed un conseguente *guadagno*.

I **parametri contabili fondamentali** di un'azienda sono:

- *Ricavo*: insieme delle entrate finanziarie conseguenti alla vendita a clienti di prodotti e servizi.
- *Spese*: insieme delle uscite finanziarie conseguenti all'acquisto di quanto serve per realizzare la funzione aziendale.

- *Guadagno*: ricavo – spese

Da un punto di vista strutturale un'azienda può avere diverse divisioni funzionali (dipartimenti, reparti, etc.) e gerarchiche (dirigenza centrale, dirigenza intermedia, dirigenza operativa e reparti operativi).

L'*organigramma* permette di schematizzare le gerarchie di un'azienda, un organigramma verticale da una visione top-down (il vertice ha la gerarchia più alta) mentre un organigramma radiale migliora la rappresentazione degli aspetti dinamici delle relazioni personali (non esiste più il concetto alto e basso).

Il *funzionigramma* racchiude e sistematizza le funzioni svolte all'interno dell'organizzazione.

Legge di Martec: la tecnologia cambia esponenzialmente ma le organizzazioni cambiano con andamento logaritmico (il gap troppo alto tra progresso tecnologico e cambiamento aziendale a volte porta al "reset" dell'organizzazione).

Oggi l'IT è "pervasiva": le normali operazioni di lavoro sono sempre più basate sull'IT anche le comunicazioni all'interno di un'azienda avvengono sempre più tramite strumenti IT/ICT.

Il **sistema informativo** è un insieme di persone, apparecchiature, procedure aziendali il cui compito è quello di produrre le informazioni che servono per operare nell'impresa e gestirla. Un sistema informativo si suddivide in:

- Risorse umane (il personale)
- Risorse tecnologiche (sistema informatica)
- Risorse organizzative (procedure, regolamenti, workflow)

L'IT è un vantaggio competitivo per le aziende? Nell'articolo IT doesn't matter di Carr si parla di come l'IT non rappresenti un vantaggio competitivo per le aziende, essa è una delle *commodities* ovvero un bene accessibile ed utilizzabile da tutti (come la ferrovia o la rete elettrica), una grande differenza risiede nei cambiamenti che l'IT subisce nel tempo rispetto alle altre utilities.

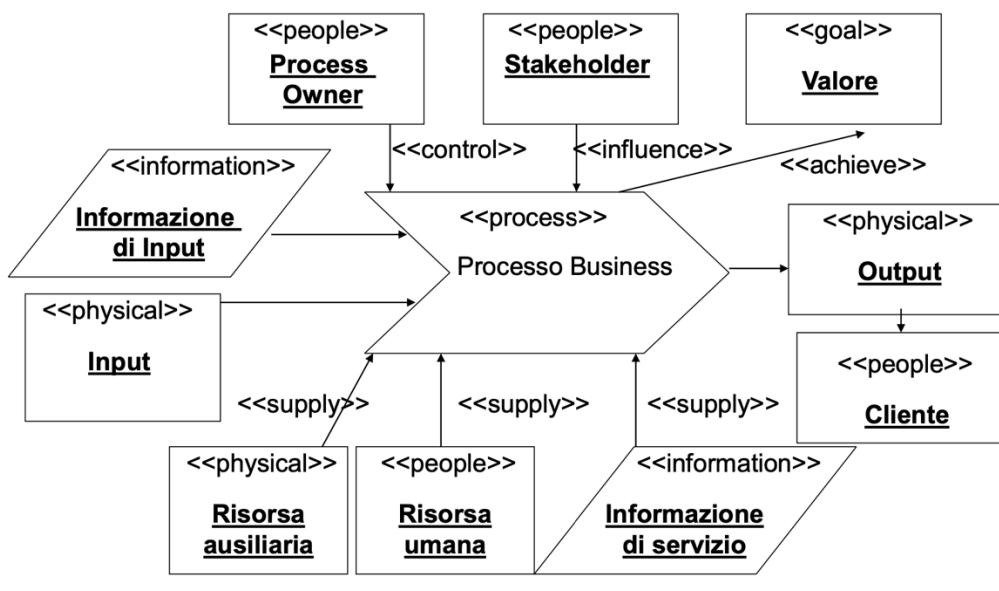
La cosiddetta "Legge di Moore" è interpretata da Carr e altri nel senso che l'inesorabile riduzione del costo dell'informatica rende l'IT una "merce", ampiamente disponibile e abbondante. La visione errata dell'IT come merce ha fatto perdere a Carr la più grande applicazione dell'IT nell'ultimo decennio: l'uso dell'IT per guidare il business dalle aziende nate sul web (lui pensava che il vantaggio competitivo della differenziazione strategica non dipendesse dall'IT).

Le "commodities" non agiscono più come meccanismo competitivo a livello di una singola azienda ma come un fattore macroeconomico, le nazioni che ritardano questi investimenti pongono le proprie industrie in difficoltà (esempio ferrovia). -> in Italia piano nazionale banda ultra-larga dal 2015 e più recente PNRR che vuole portare ad 1 Gbit/s su tutto il territorio nazionale entro il 2026, a livello regionale un esempio è la rete Lepida.

Ogni sistema è caratterizzato da uno stato, il **processo** è la successione di stati attraverso cui un sistema passa nel corso della sua evoluzione. Ogni processo si

caratterizza per l'utilizzo di input, e cioè di risorse in entrata o di partenza, e la produzione di output come risultato delle attività di quel processo.

Il **processo aziendale** è un insieme di attività che l'organizzazione svolge per realizzare un risultato definito e misurabile che trasferisce valore al fruttore del servizio e che contribuisce al raggiungimento della missione dell'organizzazione. Gli *elementi caratterizzanti* di un processo sono: gli input del processo (tipo materiale o immateriale), l'output del processo (beni materiali, servizi, informazione), risorse *ausiliarie* (entità che contribuiscono al funzionamento del processo stesso ad esempio le macchine utensili. Il software gestionale etc.), le risorse umane che compiono il processo, le risorse organizzative, le *risorse umane influenzanti* (ad esempio gli stakeholder), le *risorse umane sovraintendenti*, i costi del processo, i destinatari dell'output, il **valore aggiunto**.



↑ DA SAPERE PERCHE' LO CHIEDE ↑

Da un punto di vista analitico il *business process* può essere definito come una tupla BP (A, I, O, C) dove:

- A sono le attività, formate da una serie di azioni fisiche o decisioni manageriali
- I sono gli input del processo, formati da materie prime o risorse aziendali
- O sono gli output del processo, formato da beni materiali o immateriali
- C sono i clienti, ovvero i destinatari dell'output del processo.

In alternativa la tupla può essere definita come BP (C, R, A, S, O)

- C = clienti
- R = richiesta, un processo è avviato da almeno una richiesta emessa da un cliente
- A = attività, formate da una serie di azioni fisiche o decisioni manageriali
- S = organizzazione, riuniscono gli attori che sono coinvolti nel processo
- O = output del processo, formato da beni materiali o immateriali.

L'output di un processo può costruire l'input di un processo successivo (così come l'input di un processo può essere l'output di quello precedente), inoltre, il cliente non deve essere per forza esterno ad un'azienda (basti pensare ad un'unità organizzativa dell'impresa stessa che utilizza il risultato di un processo come input per lo svolgimento di altri processi). Il processo non è altro che una *catena di attività attraverso le quali partendo da determinati input, si ottengono output voluti*.

Un'attività è caratterizzata dal suo costo, dal tempo di svolgimento e dalla qualità dell'output finale; questi elementi costituiscono una misura dell'efficacia ed efficienza con cui si svolge il processo. Un processo che possiede queste caratteristiche è un processo che crea valore perché è in grado di offrire al cliente un *beneficio superiore alle risorse impiegate*.

La definizione **ITIL** (insieme di linee guida ispirate dalla pratica nella gestione dei servizi IT) di processo è “insieme di *attività coordinate* rivolte ad un compito/scopo specifico, per produrre un *risultato* che direttamente o indirettamente crea *valore* per il *cliente*”. Un processo, quindi, deve essere *misurabile* (i manager misurano i costi e le qualità mentre gli operatori sono interessati a durata e produttività), avere *risultati specifici*, avere *uno o più clienti*, rispondere ad *eventi specifici*.

Il **controllo di un processo** è l'attività di pianificazione e regolazione di un processo, al fine di eseguirlo in modo efficace, efficiente e costante. Ogni processo va assegnato un *process owner*, il quale è responsabile per il conseguimento degli obiettivi attesi (efficienza = output effettivo/input, mentre efficacia= output effettivo/output atteso).

Il **flusso informativo** di un processo è il flusso di informazioni associato ad un processo che passa attraverso e tra le fasi, se il flusso informativo è completamente realizzato tramite strumenti IT si può definire *flusso informatico*.

Classificazioni dei processi aziendali

I **processi primari** creano direttamente un valore riconosciuto dal cliente esterno (produttivi, logistici e di vendita), i **processi secondari** (o di supporto) servono per la realizzazione dei processi primari ma non creano di per sé un valore riconosciuto dal cliente esterno (es. di processi secondari sono l'amministrazione, la finanza, la pianificazione etc.).

I livelli di un processo primario sono la pianificazione operativa (che può essere di lungo o breve periodo), l'esecuzione, la rilevazione e il monitoraggio ed infine il controllo.

Un'altra classificazione dei processi è fornita dalla **piramide di Anthony** che suddivide i processi in:

- *Processi direzionali (strategici)*: concorrono alla definizione degli obiettivi strategici
- *Processi gestionali (tattici)*: traducono gli obiettivi strategici in obiettivi economici e ne controllano il raggiungimento

- *Processi operativi*: concorrono alla attuazione degli obiettivi

	Amministrazione comunale	Banca	Azienda
Processi strategici	Verifica di costi e ricavi dei servizi sociali, definizione di nuove tariffe, piani regolatori	Verifica dell'andamento di un servizio, decisione di aprire nuovi servizi	Scelta delle aree di mercato più convenienti
Processi gestionali	Controllo dei pagamenti, solleciti, confronti mensili tra entrate previste ed effettive, monitoraggio dell'inquinamento	Revisione degli scoperti	Controllo scostamento settimanale tra preventivo e consuntivo
Processi operativi	Contabilizzazione dei pagamenti dei cittadini, manutenzione delle strade	Gestione dei movimenti dei conti concorrenti	Registrazione costi delle commesse

La **classificazione di Porter** considera l'intera attività aziendale come un *macro-processo*, suddividendo i processi in:

- *Processi di input -> buy side*
- *Processi di azione interna -> inside*
- *Processi di output -> sell side*

Porter teorizza la **catena del valore**, l'attività di un'azienda può essere vista come una sequenza di attività finalizzata a produrre valore per il cliente, il valore è il prezzo che il cliente è disposto a pagare per il servizio o per il prodotto che gli viene fornito. La catena del valore fornisce una "visione a flusso" mentre la piramide di Anthony fornisce una "visione gerarchica".

Una classificazione generale delle attività svolte in un'azienda è composta da:

- *Comprendere dei mercati e dei consumatori* (determinazione dei bisogni dei clienti, misurazione della soddisfazione dei clienti, controllo dei cambiamenti e delle aspettative del mercato, etc.).
- *Sviluppo visione e strategia* (controllo dell'ambiente esterno, definizione della strategia e della struttura organizzativa, sviluppo e definizione degli obiettivi etc.)
- *Sviluppo prodotti e servizi* (ingegnerizzazione e gestione del processo di sviluppo di nuovi prodotti)
- *Marketing e vendite*
- *Produzione e consegne per imprese manifatturiere* (pianificazione e acquisizione delle risorse. Gestione dei processi produttivi e delle consegne)
- *Produzione e consegna per imprese di servizi* (pianificazione ed acquisizione delle risorse, erogazione dei servizi)
- *Fatturazione e servizi al cliente* (fatturazione ai clienti)
- *Gestione informazioni* (valutazione e controllo del sistema informativo)

- *Sviluppo gestione risorse umane* (elaborazione strategie/risorse umane, formazione del personale, riallocazione del personale, gestione ambiente lavorativo etc.)
- *Gestione risorse fisiche e finanziare*
- *Realizzazioni programmi tutela ambientali* (formulazione delle strategie ambientali, educazione del personale etc.)
- *Gestioni relazioni esterne* (comunicazione con gli stakeholders)
- *Gestione miglioramento e cambiamento*

La **scomposizione sequenziale dei processi** dettaglia i processi per successivi livelli di approfondimento: si parte dal *macro-processo*, primo livello di segmentazione di un'azienda, i clienti possono essere esterni ed interni all'azienda stessa, sia input che output sono ben definiti (esempio progettazione e design di prodotti). Il *processo* serve ad illustrare in modo dettagliato le operazioni di un'azienda: la *disaggregazione* avviene quando un macro-processo viene scomposto nei processi che lo compongono, la *raffinazione* è la specializzazione di un processo generico; i processi hanno come clienti altri processi.

La *fase* ha lo scopo di descrivere il modo con cui un processo è implementato, si compone in una più *attività*. Le *attività* sono il livello minimo di analisi normalmente considerato, sono determinate scomponendo i processi secondo una logica sequenziale. Producono un output ben definito ma con valore solo interno al contesto aziendale, sono considerate atomiche (non ulteriormente scomponibili).

L'azienda: visione per funzioni vs visione per processi

L'insieme dei processi viene compiuto dalle risorse umane presenti nelle varie *divisioni aziendali*. Le **funzioni** (aziendali) sono aggregazioni di uomini e mezzi necessari per lo svolgimento di un'attività della stessa natura, esempi sono la funzione acquisti, vendite, produzione, amministrativa etc. L'intera azienda viene suddivisa in unità organizzative funzionali che potranno suddividersi in reparti e/o uffici (ad esempio funzione amministrativa divisibile in ufficio clienti, ufficio contabilità, ufficio fornitori ecc.).

I **processi** sono formati anche da attività di natura diversa, ma sono finalizzate al raggiungimento dello stesso output: un processo attraversa più funzioni (o più funzioni concorrono alla realizzazione di un unico processo).

L'organizzazione delle aziende per funzioni spesso causa inefficienze in quanto i processi potrebbero non essere codificati esplicitamente -> esempio gestione di un ordine. Una visione per processi ha come obiettivo generale la creazione del valore, facilitando la realizzazione di obiettivi di profitto e monitoraggio della performance di costo.

Gli *elementi chiave della business process orientation* sono:

- La progettazione e documentazione dei processi aziendali

- L'impegno della direzione verso l'orientamento al processo
- Proprietà del processo
- Misurazioni delle prestazioni del processo
- Cultura aziendale con l'approccio del processo
- Applicazioni di miglioramento continuo del processo
- Struttura organizzativa orientata al process

Il **business process management (BPM)** è una metodologia utilizzata dalle organizzazioni per migliorare continuamente i processi di business operative (migliore agilità del process, allineamento del processo con le “best practices” dell’industria, miglioramento dell’efficienza del processo).

Il BPM consiste in un ciclo continuo con quattro fasi:

1. Definire e mappare il processo di business
2. Identificare i modi per migliorare quelle fasi/attività del processo che aggiungono valore
3. Identificare modi per eliminare o consolidare fasi/attività del processo che non aggiungono valore
4. Creare o adattare workflow informatici per farli corrispondere alle mappe migliorate del processo

Il **workflow** è un’automatizzazione di un processo aziendale, per intero o di una sua parte, durante la quale i documenti, le informazioni o i tasks sono passate da un partecipante ad un altro per azione, basandosi su un insieme di regole procedurali. Con il termine *business process automation* si intende la creazione o l’adattamento dei workflow informatici per farli corrispondere alle mappe migliorate del processo. Con il termine *business process improvement* si intende lo studio dei processi di business, la creazione di nuovi processi (o riprogettazione) per migliorare i workflow e/o utilizzare nuove tecnologie che abilitano nuove strutture dei processi.

La *business process reengineering* consiste in una totale revisione dei processi.

BPM: principi e pratiche: l’obiettivo è quello di migliorare i prodotti e servizi attraverso un *approccio strutturato* centrato sulla progettazione e la gestione strutturale dei processi di business dell’azienda.

Principi: i processi aziendali sono *asset aziendali* che sono centrali nel creare valore per i clienti, misurando e analizzando i processi di business un’azienda può fornire valore consistente ai clienti e ha la base per il miglioramento dei processi.

I processi aziendali dovrebbero essere continuamente migliorati e l’IT è un *enabler essenziale* per il BPM.

Pratiche: impegnarsi per una struttura organizzativa orientata ai processi, nominare i process owners, i manager senior devono impegnarsi e guidare il BPM (il suo miglioramento dovrebbe avere un approccio “bottom-up”), mettere in atto sistemi IT per monitorare, controllare, analizzare e migliorare i processi.

Lavorare in modo collaborativo con i business partner sui processi interaziendali, formare continuamente la forza lavoro e migliorare continuamente i processi

aziendali. Di fondamentale importanza è utilizzare sia *metodologie incrementali (Six Sigma)* e più radicali (es. BPR) per implementare il miglioramento dei processi.

Six Sigma nasce in ambito produzione (Motorola), si concentra sulla minimizzazione dei difetti, ha una forte enfasi sulla misurazione dell'output dei processi, specialmente in termini di qualità.

Lean nasce in ambito produzione (Toyota), vuole eliminare gli sprechi: le attività che non aggiungono valore per il cliente. Il BPM pone più enfasi sull'utilizzo dell'IT come strumento per migliorare i processi di business e per renderli più costanti e ripetibili.

APPROFONDIMENTO 3 WAVES DELLA PBM: 1° wave -> i processi impliciti alle work practices e messi da parte nei manuali. 2° wave -> processi possono essere reingegnerizzati manualmente attraverso un'attività one-time (nascita delle applicazioni ERP) 3° wave -> abilita le aziende e i lavoratori a creare ed ottimizzare i nuovi processi business mediante processi business agili, è la sintesi e l'estensione di tutte le tecnologie come la BPR.

I **BPMS (business process management systems)**: suite software che supportano gli analisti di business e gli sviluppatori IT, implementanti per modellare, simulare, automatizzare e monitorare i processi; includono i motori di workflow e di EAI.

Le nuove tecnologie per il miglioramento dei BP sono: *process mining*, si riferisce all'uso di una serie di tecniche per analizzare i log degli eventi dei processi aziendali al fine di comprendere meglio i processi aziendali e renderli più efficienti. La *robotic process automation* è uno strumento di produttività che permette all'utente di configurare uno o più script per attivare le sequenze di tasti in modo automatico -> i bot sono utilizzati per imitare o emulare compiti selezionati all'interno di un processo aziendale o informatico.

L'*intelligent BPMS* combina il BPM con l'intelligenza artificiale per creare rapidamente esperienze di flusso di lavoro dinamiche, dall'inizio alla fine, attraverso una piattaforma basata sul cloud.

La trasformazione dei processi deve integrare sia l'*innovazione tecnologica* che l'*innovazione organizzativa*. Bracchi individua 4 **variabili organizzative**:

1. L'organizzazione del processo
2. Il flusso delle attività
3. Le competenze delle risorse umane
4. Il sistema di misurazione e controllo delle prestazioni

Sono variabili interrelate (esempio adozione di sistemi di ordinazione via web)

Gli elementi principali dell'**organizzazione del processo** sono: l'*organigramma* rappresenta la gerarchia delle responsabilità e delle autorità nell'organizzazione. Le *tabelle delle proprietà* forniscono una descrizione del mandato, un elenco dei compiti assegnati e dei processi svolti e *LRC o RACI* -> specificazione dei ruoli e delle strutture nei processi.

Il **flusso delle attività** è la sequenza delle attività attraverso cui è svolto il progetto, determina la durata del processo, le informazioni che appartengono al flusso è il tipo

di attività svolto, la sequenza delle attività e gli attori (e gli oggetti) che le svolgono. È di significativa importanza l'utilizzo della tecnologia. (ESEMPIO sulla registrazione del voto degli esami, prima con registrazione su moduli cartacei, poi su moduli a lettura ottica ed infine con registrazione in tempo reale).

Le **risorse umane** determinano la differenza fra il risultato effettivo ed il massimo teoricamente possibile in una data configurazione di processo.

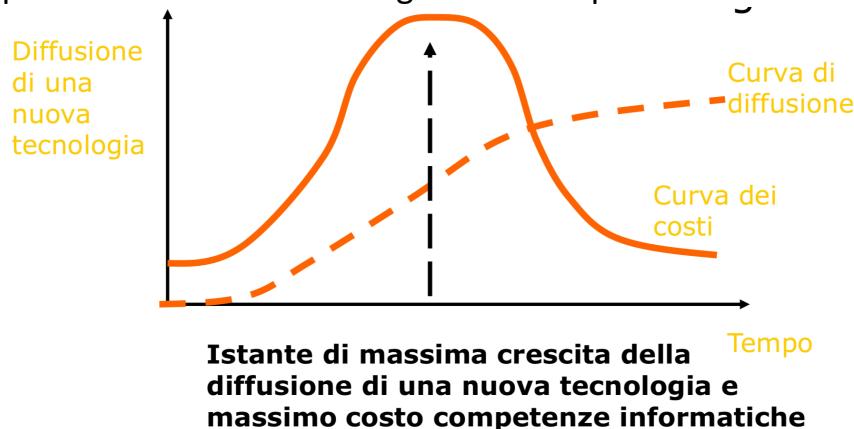


Grafico sul ruolo delle risorse umane sull'importanza dell'introduzione nelle nuove tecnologie.

I processi sono governati da un sistema di **misurazione delle prestazioni**: ad esempio il rivelamento dei costi e della soddisfazione del cliente. È necessario implementare un sistema di incentivazione e di promozione, per lavorare per obiettivi: indicando alla dirigenza gli obiettivi da raggiungere e alle forze di vendita gli obiettivi di budget. La *definizione della scala dei valori* è un processo orientato al cliente per garantirne la sua soddisfazione. I **KPI** sono i parametri fondamentali, alcuni esempi di KPI sono le vendite (numero di contratti firmati nel periodo, importo complessivo dei contratti nel periodo), i clienti (numero di clienti fidelizzati, quota di mercato detenuta), operativi (tempo di completamento ordini, tasso soddisfazione clienti).

Il **ciclo di Deming (Plan Do Check Act)** è alla base del Business process

Reengineering: è un ciclo iterativo per il miglioramento di processi e prodotti. Si parte pianificando interventi su tutto ciò che può essere utile per migliorare i processi, successivamente si esegue ciò che viene pianificato e se ne verificano i risultati ed infine vengono attuate delle correzioni su quanto attuato per migliorare i risultati.

La reingegnerizzazione dei processi aziendali

Per migliorare i processi aziendali ci sono due alternative:

Business process Improvement (BPI): interventi di tipo incrementale cioè volti al continuo e graduale miglioramento dei processi.

Business process Reengineering (BPR): interventi di tipo radicale, cioè volti al completo ridisegno del processo.

Per quanto riguarda la reingegnerizzazione le fasi principali su cui si basano le rielaborazioni delle *variabili organizzative* sono:

1. Rilevazione della situazione esistente

- 1.1. *Identificazione dei macro-processi*, seguendo un preciso modello (es. catena del valore) per identificare i clienti, l'input e l'output di un processo.
- 1.2. *Disaggregazione dei processi* per un'analisi più approfondita (costruzione di diagrammi gerarchici, di flusso e descrizione strutturata delle proprietà dei processi).
- 1.3. *Analisi delle unità organizzative* (utilizzando tabella LRC/RACI)
- 1.4. *Valutazione dei processi*: definire i parametri di funzionamento e il giudizio sui valori dei prodotti (esecutori valutano tempi necessari per svolgere il processo e le risorse dedicate ad esso mentre i clienti valutano la qualità e il valore del prodotto)

2. Confronto con le altre realtà

- 2.1. *Confronto quantitativo e parametrazione*, si sceglie un insieme adeguato di parametri e si effettua un confronto quantitativo con situazioni simili
- 2.2. *Confronto qualitativo*, analizzando delle cause di diversità del servizio e confrontando modelli organizzativi e tecnologici

3. Riprogettazione dei processi

- 3.1. *Rappresentazione sintetica degli elementi della soluzione proposta*
- 3.2. *Riorganizzazione basata su processi best practice* (uso di tabelle as-is/to-be)

ESEMPIO REINGEGNERIZZAZIONE DI UN PROCESSO: CASO OTICON

Oticon è un'azienda di apparecchi acustici che nella metà negli anni 80 subì gravi perdite economiche in quanto il mercato preferiva apparecchi di qualità mediocre ma interni all'orecchio (rispetto a quelli di ottima qualità ma esterni di Oticon), dopo un periodo iniziale di tagli ai costi viene introdotta una nuova *vision*: i clienti di riferimento diventano direttamente i portatori di apparecchi acustici e non le cliniche specializzate -> organizzazione basata su progetti, attraverso un processo di informatizzazione e reingegnerizzazione dei processi. La *struttura funzionale* fu rimpiazzata da un'organizzazione basata su gruppi di progetto (team leader scelto dalla direzione aziendale, altri partecipanti del gruppo su scelta volontaria), altri interventi sono stati: la sostituzione di archivi cartacei con archivi elettronici, nuovi meccanismi di incentivazione e retribuzione, eliminazione di ogni status symbol, nuovi meccanismi di retribuzione, passaggio da CED ad architettura di rete Client-Server e cambio delle postazioni di lavoro introducendo open-space con postazioni uguali con cassetiera mobile per spostarsi in un nuovo gruppo.

Capitolo 2 – I sistemi informativi di supporto operativo e direzionale

La risorsa informazione e la piramide DIKW

L'informazione è l'oggetto del lavoro del sistema informativo, è la principale risorsa scambiata, selezionata ed elaborata nelle attività gestionali di coordinamento e controllo. È una risorsa immateriale, ed è la base della *conoscenza, esperienza individuale, esperienza organizzativa*. L'informazione non viene distrutta dall'uso e permette la creazione di nuova conoscenza, inoltre non è facilmente misurabile.

La **piramide DIKW** fornisce una rappresentazione gerarchica dell'informazione, alla base ci sono i *dati*: materiale informativo grezzo, possono essere scoperti, raccolti o prodotti dal mondo reale. L'*informazione* è al gradino superiore, viene costruita dai dati elaborati cognitivamente (ponendoli in relazione reciproca ed organizzandoli mediante dei pattern), salendo di livello troviamo la *Conoscenza*: è l'informazione esplicita, che si acquisisce attraverso l'*esperienza* -> è fondamentale un livello di comunicazione partecipatorio. La punta della piramide è costituita dalla *saggezza*: il livello di comprensione più indefinito ed intimo, è il risultato di contemplazione, valutazione, interpretazione (processi strettamente personali), non può essere condivisa come avviene per la conoscenza.

La spirale della conoscenza indica i diversi approcci per condividere conoscenza: *socializzazione*: persone diverse che interagiscono (da conoscenza tacita a conoscenza tacita)

esteriorizzazione: da conoscenza tacita ad esplicita tramite una formalizzazione

combinazione: da conoscenza esplicita a conoscenza esplicita (tramite elaborazioni o trasferimenti)

interiorizzazione: da conoscenza esplicita a conoscenza tacita (tramite apprendimento)

Sistema informatico e applicazioni

Un sistema informativo (IS) può essere scomposto su base funzionale, strutturale, rispetto all'utenza o per combinazione di queste parti.

Una possibile stratificazione è data da:

- *Software applicativo*: applicazioni per end user che svolgono operazioni sui dati
- *Software infrastrutturale*: servizi software per il livello superiore (web server, DBMS)
- *Sistemi operativi*
- *Infrastruttura: HW + rete*

Una **transazione** è definita come un'unità logica di elaborazione, ovvero una sequenza di operazioni che hanno un effetto globale sul database.

Le proprietà **ACID** delle transazioni sono:

- **Atomicity:** tutte le operazioni della sequenza terminano con successo, se fallisce una di esse fallisce l'intera transazione.
- **Consistency** una transazione è una trasformazione corretta dello stato del database.
- **Isolation:** l'effetto di esecuzioni concorrenti di più transazioni deve essere equivalente ad una esecuzione seriale delle stesse (transazioni concorrenti non devono influenzarsi reciprocamente).
- **Durability:** gli effetti sulla base di dati prodotti da una transazione terminata con successo sono permanenti.

Una transazione può essere *Committed* (operazioni eseguite con successo -> database si trova in un nuovo stato) o *Aborted* (alcune operazioni non possono essere portate a termine -> database ritorna all'ultimo stato consistente).

Sistema informatico e applicazioni

Distinguiamo diversi tipi di sistemi informatici, ognuno di essi serve un gruppo distinto del business.

- **I sistemi informativi operativi** supportano i manager e gli addetti operativi per registrare il flusso delle transazioni entro l'azienda (es. vendite, incassi, paghe etc.)
- **I sistemi informativi per gestione conoscenza** supportano i knowledge workers nella creazione di nuova conoscenza gestendo i flussi di dati.
- **I sistemi di supporto dell'attività manageriale** favoriscono le attività di controllo, monitoraggio ed amministrative dei *middle manager*, fornendo report periodici.
- **I sistemi di supporto dell'attività strategiche** aiutano i *senior manager* ad affrontare problemi strategici e le tendenze a lungo termine.
- **I transaction Processing Systems (TPS) sono** sistemi di base che servono il livello operativo dell'azienda (registrazioni ordini, prenotazioni alberghiere, etc.). Sono designati per l'utilizzo da parte del personale operativo e dei supervisor.
- **I sistemi per l'ufficio** aumentano la produttività dei lavoratori su documenti e dati (fogli elettronici, elaborazione di testi etc.), sono tipicamente utilizzati dagli impiegati.
- **Knowledge Working Systems (KWS)**, servono alla gestione e alla creazione di nuova conoscenza, sono i sistemi di progetto come, ad esempio, CAD; usati da professionisti e staff tecnico.
- **Management information systems (MIS)**, servono principalmente le funzioni di pianificazione e controllo, supportano le decisioni a livello manageriale; usati dai *middle manager*.

- **Decision support systems (DSS)**, rispondono anche essi alle esigenze del livello manageriale dell’azienda, aiutano a prendere decisioni in contesti non unici o nuovi per l’azienda.
- **Executive support systems (ESS)** rispondono alle necessità di livello strategico delle aziende. Riguardano decisioni non di routine che richiedono valutazioni, giudizi, conoscenze approfondite possono essere sistemi programmabili (basati su regole), automatici (richiedono una fase di addestramento), e infine sistemi ibridi; sono destinati ai *senior manager*.

Per quanto riguarda la **scomposizione in aree funzionali** si distinguono:

- **Vendite e marketing**: elaborazione ordini (livello operativo), analisi di mercato (livello conoscenza), determinazione dei prezzi (livello manageriale), previsioni delle tendenze di vendita (livello strategico).
- **Produzione**: controllo delle macchine (livello operativo), CAD (livello conoscenza), pianificazione della produzione (livello manageriale), individuazione degli impianti (livello strategico).
- **Gestione finanziaria e contabilità**: gestione incassi (livello operativo), analisi di portafoglio (livello conoscenza), budget (livello manageriale) e pianificazione dei profitti (livello strategico)
- **Risorse umane**: addestramento e sviluppo (livello operativo), gestione carriere (livello conoscenza), retribuzioni (livello manageriale) e pianificazione delle risorse umane (livello strategico)

Nelle aziende strutturate per processi i flussi informatici coinvolgono diverse divisioni, si integrano (o acquistano) nuovi sistemi integrati. Per il passaggio ai sistemi integrati occorre un coordinamento di attività, decisioni e conoscenza nell’ambito delle varie funzioni e dei livelli e delle unità operative dell’azienda.

I sistemi integrati di gestione: gli ERP

ERP (Enterprise Resource Planning) è un sistema IT integrato per la gestione, copre tutti i processi più importanti di un’azienda (acquisti, vendite, logistica, contabilità, gestione risorse umane etc.). Per essere considerato un software ERP l’integrazione deve avvenire in tempo reale senza aggiornamenti batch periodici, tutte le applicazioni devono accedere ad un solo database per impedire che i dati siano ridondanti, tutti i moduli devono avere lo stesso aspetto (UI), gli utenti dovrebbero essere in grado di accedere a qualsiasi informazione nel sistema senza bisogno di lavoro di integrazione da parte del dipartimento SI.

La base di dati condivisa minimizza i dati da immettere e permette un aggiornamento coerente di più informazioni, la tipica architettura fisica di un ERP è di tipo *Client-Server 3-tier* (presentazione, applicazione e database).

Modelli di ERP più noti sono SAP R/2 (basato su mainframe) SAP R/3 (client server), SAP ERP e più recentemente S/4.

SAP R/3 (system analysis and program development) fornisce una serie di ambienti che sono costituiti da un insieme di applicazioni chiamate applicazioni R/3, sono di tipologie diverse e le più importanti sono le applicazioni client. Le applicazioni Client sono tutte le applicazioni che possono essere sviluppate per interrogare il sistema gestionale per effettuare una o più transazioni, i linguaggi con cui possono essere scritte tali applicazioni sono il linguaggio proprietario ABAP oppure C, C++, Java etc. Il *middleware* è costituito dall'insieme di tecnologie di interfaccia che permette di mettere in comunicazione il sistema SAP R/3 sia con hardware e software di base e sia con le applicazioni R/3. (es. dialogo sistema SAP ed un Database mediante comandi SQL standard).

Le fasi di implementazione di un SAP in azienda sono:

- **Project preparation:** i decision makers definiscono un piano di obiettivi chiaro ed un approccio efficiente per raggiungerli, l'ordine di progettazione è creato e la strategia di implementazione ben definita. In questa fase si determinano i requisiti del sistema, una strategia per i clienti, una strategia di rilascio e un sistema di trasporti.
- **Target Concept** viene creato il *Business Blueprint* (documentazione dell'implementazione SAP ERP)
- **Realization** viene personalizzato il sistema SAP ERP per soddisfare al meglio i requisiti business
- **Production preparation** vengono effettuati test sul sistema, ed un addestramento per gli utenti che lo dovranno utilizzare
- **Production Start-Up** in questa fase i progetti successivi sono già in corso d'opera per implementare nuove componenti dell'applicazione o automatizzare e migliorare i processi di business.

Nel mercato attuale è disponibile **SAP HANA CLOUD PLATFORM**, costituita da building blocks (UI, Business Logic, Persistency, Connectivity), è un'architettura 2 tier dove l'utente si connette ed è autorizzato direttamente da HANA (la sicurezza è gestita dal database).

Per quanto riguarda il mercato degli ERP alcune alternative sono E-business suite di Oracle, Microsoft Dynamics 365, Ad Hoc di Zucchetti (italiana). WebERP ed Openbravo sono delle versioni open source di ERP.

CRM: Il customer relationship management

Il CRM è un sistema di interazione con i clienti composto da metodologie, software e funzionalità internet, che integra i dati provenienti da diversi canali di contatto in un'unica base dati condivisa da più aree dell'azienda (marketing, vendite, customer service). L'impresa costruisce una base di dati sui propri clienti, in questo modo la direzione ed i rappresentati del servizio clienti possono accedere alle informazioni, i clienti possono soddisfare le loro esigenze con piani di prodotto e di offerte ed

inoltre l'azienda può sapere quali prodotti un cliente ha acquistato e ricordare ai clienti le esigenze del servizio.

Esistono diversi tipi di CRM:

CRM OPERATIVO: deve sostenere il cosiddetto “front office” dei processi di business, che includono il contatto con il cliente.

CRM ANALITICO i dati raccolti nell’ambito del CRM operativo vengono analizzati per segmentare i clienti e ideare offerte e campagne di marketing. (raccolta ed analisi sono un processo permanente ed iterativo)

CRM COLLABORATIVO consente a tutte le aziende lungo il canale di distribuzione di lavorare e condividere informazioni sui clienti.

CRM STRATEGICO/DIREZIONALE ottiene ed utilizza sintesi di informazioni per la direzione commerciale.

Le *fasi del CRM* sono:

1. **Identificare e segmentare i propri clienti** e valutarne il valore attuale e prospettico.
2. **Differenziare le offerte e le campagne di marketing** in funzione del profilo dei clienti target, della redditività attesa e del costo delle azioni ideate.
3. **Interagire**, in questa fase si entra nella dimensione operativa del CRM, che comporta l'esecuzione materiale delle campagne/azioni di marketing prescelte.
4. **Apprendere e personalizzare**, in questa fase si qualifica e distingue un qualsiasi sistema di analisi dei clienti da un processo in ottica CRM: il sistema tattica la risposta positiva o negativa dei clienti contattati ai fini di apprendere e adattare progressivamente la propria offerta alle esigenze personalizzate di ciascun segmento di clienti. (in questa fase sono contenute anche le azioni impreviste da parte di clienti).

Uno dei risultati più importanti del CRM è quello di ottimizzare l'interazione con i clienti indirizzando il giusto messaggio, al giusto cliente al tempo opportuno attraverso il giusto canale. Il punto di partenza nella definizione della strategia di marketing è, l'analisi dei bisogni del cliente. La differenza è la disponibilità di strumenti informatici che ampliano le possibilità di azione.

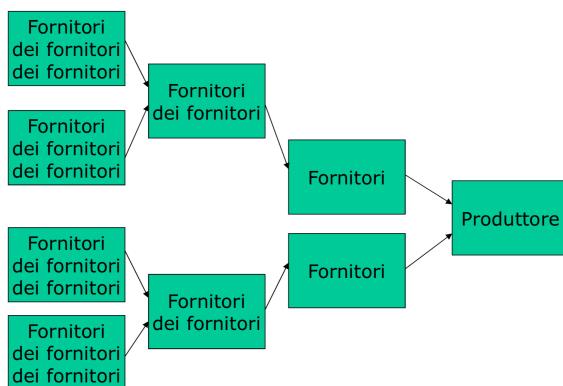
Nel *marketing one to one* si possono identificare i clienti dell'impresa, classificare i clienti in gruppi omogenei, sviluppare sistemi di interattività con i clienti e personalizzare l'offerta di prodotti e servizi.

L'avvento del web ha portato ad un'evoluzione delle tecniche CRM -> observation del cliente sul sito web e campagne mirate di e-mailing, un esempio di software di gestione contatti è il *Prometeo information manager* (gestione anagrafiche, gestione recapiti, gestione eventi, gestione documenti, gestione associazioni).

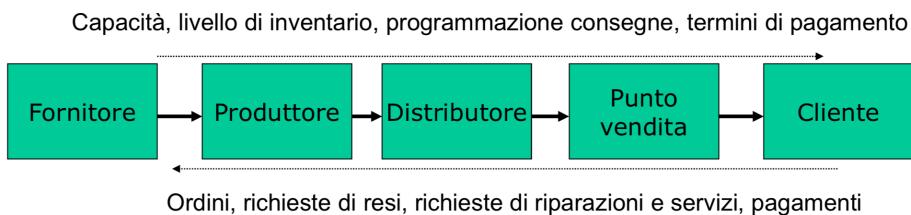
Il Supply Chain Management

È la gestione dei sistemi di fornitura, si occupa del collegamento e del coordinamento delle attività relative ad acquisti, creazione e trasferimenti di un prodotto. I *processi di fornitura* formano una rete di processi sia decisionali che operativi che consentono di procurarsi materiali, trasformare materiali grezzi in prodotti semilavorati e finiti e di distribuire prodotti finiti ai clienti.

SCM: schema dei processi a monte



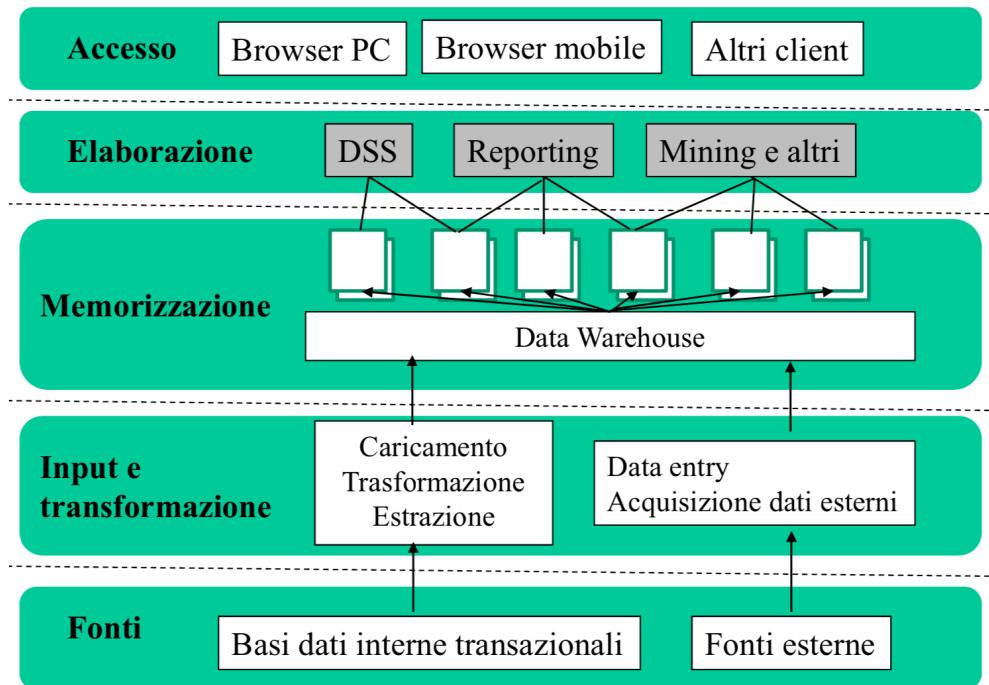
SCM: schema dei processi a valle



Il software SCM deve aiutare a decidere cosa produrre e quando produrlo, cosa trasferire (come e quando) ed infine cosa immagazzinare (dimmi dove e quando!!) Alcuni compiti di un software SCM sono: comunicare rapidamente lo stato degli ordini, monitorare lo stato degli ordini, controllare la disponibilità ad inventario ed i livelli di inventario, aiutare a ridurre i costi di inventario, pianificare la produzione sulla base delle richieste dei clienti e comunicare rapidamente i cambiamenti nel progetto dei prodotti.

La Business Intelligence e normalizzazione basi di dati

La *business intelligence* comprende l'insieme di applicazioni e tecnologie per l'analisi dei dati, comprende DSS, OLAP. Analisi statistiche, data mining e modelli previsionali, sistemi reportistica direzionale e cruscotti aziendali.



Può capitare che per colpa di errori di schematizzazione o durante la rianalisi di database vecchi scarsamente documentati ci siano delle ridondanze (ad esempio si ripete più volte che un impiegato percepisce un certo stipendio) o delle anomalie (nell'aggiornamento/cancellazione/inserimento di nuovi dati). Per questo motivo viene introdotta la **dipendenza funzionale**, che è un vincolo di integrità per il modello relazionale. Data una relazione R definita su uno schema S(X) e due sottoinsiemi di attributi Y e Z non vuoti di X, esiste una dipendenza funzionale Y->Z, se per ogni coppia di tuple t1 e t2 aventi lo stesso valore di Y risulta che hanno lo stesso valore di Z.

Schemi E/R corretti producono in generale buoni schemi relazionali senza problemi di anomalie e ridondanze.

OLTP, *On-Line Transaction Processing* è un insieme di tecniche software utilizzate per la gestione di applicazioni orientate alle transazioni. Il database per l'OLTP deve essere normalizzato completo, avere un alto numero di tabelle ed associazioni, le interrogazioni richiedono join di molte tabelle ed inoltre la struttura dei dati non varia di frequente.

Passando da un sistema transazionale (OLTP) ad un sistema di analisi **OLAP** (*On-Line Analytical Processing*), cambiano le caratteristiche di:

- Normalizzazione
- Prestazioni su query e modifica dei dati
- Profondità storica
- Complessità delle query
- Dettaglio degli eventi rilevati

L'**ETL (Extract Transform and Load)** è il processo di raccolta dei dati da un numero illimitato di sorgenti e della loro successiva organizzazione e centralizzazione in un unico repository, consiste in tre fasi:

- *Fase di estrazione* dal database di produzione
- *Fase di trasformazione* nella rappresentazione più adatta all'analisi da effettuare
- *Fase di caricamento* dei dati nel database del programma di analisi

L'**ELT (Extract, Load and Transform)** è un'alternativa più recente all'ETL. I dati vengono caricati nel data store target prima della trasformazione, in questo modo viene offerta una maggiore flessibilità (i data warehouse basati sul cloud consentono di lavorare su dati strutturati e dati non strutturati). Le soluzioni ELT sono generalmente SaaS basate su cloud, disponibili per un maggior numero di clienti (ETL può richiedere molte risorse); l'ELT consente la trasformazione dei soli dati interessati riducendone i tempi di trasformazione, mentre con l'ETL i tempi possono aumentare drasticamente. Per quanto riguarda la manutenzione l'ELT lascia i dati originali intatti e già caricati nel caso in cui sia necessaria un'ulteriore trasformazione.

Le caratteristiche di un database per un ambiente analitico (**OLAP**) sono:

- Entità denormalizzate
- Disegno del database più semplice per una comprensione più facile da parte dell'utente
- Le interrogazioni richiedono più join
- Ottimizzato per la consultazione di grandi moli di dati (per l'utente finale è normalmente in sola lettura)

Il **Data warehouse** può essere considerato come un db Read-only, un "magazzino di dati" a livello di impresa, è un insieme di strumenti per convertire un visto insieme di dati in *informazioni* utilizzabili dall'utente. Le informazioni devono essere accessibili in maniera veloce, i dati dell'azienda sono quindi centralizzati in un unico database ed offrono un valido supporto per l'analisi dei dati.

Il **Data mart** è un "magazzino di dati" a livello dipartimentale, ovvero un segmento di un data warehouse -> struttura fisica uguale a quella di un data warehouse ma con finalità più ristrette (i dati coprono solo alcune aree aziendali, minori costi di realizzazione e risultati più vicini nel tempo).

Il data warehouse garantisce maggiore coerenza dei dati sebbene il costo sia maggiore, è possibile ricavare dei Data Mart da un Data Warehouse (approccio top-down) ma anche un Data Warehouse unendo più Data Mart (approccio bottom-up). Le caratteristiche principali di un Data Warehouse sono: subject oriented, integrato, non volatile e che varia nel tempo.

Esistono dei modelli generici pensati per queste esigenze:

- Schema a stella (non normalizzato "perché sono riportati attributi che esprimono dipendenze funzionali che esplicitano la chiave (più comprensibile ma inefficiente e più sensibile a

ridondanze e/o altri problemi sui dati)”) è preferibile nei data mart, viene usato per semplificare l’analisi e la comprensione degli utenti business.

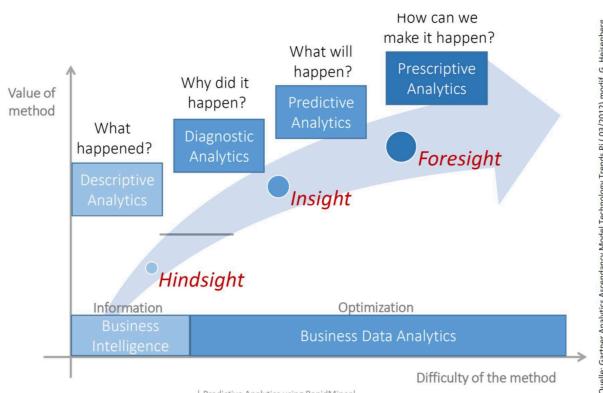
- Schema a fiocco di neve (normalizzato) utilizza meno spazio di memorizzazione e riduce il rischio di anomalie di aggiornamento, lo svantaggio sono i join complessi

Un’*analisi di dati* ha come risultati delle: *associazioni* (situazioni connesse ad un unico evento), *sequenze* (eventi connessi da relazioni temporali), *classificazioni* (suddivisioni in gruppi ove valgono regole), *raggruppamenti* (definizioni di gruppi non noti a priori), *previsioni* (uso dei dati esistenti per scoprire dati futuri).

ESEMPIO SOCIETA’ DELLA GRANDE DISTRIBUZIONE (tratto da Bracchi):

SI operativo registra ingressi, stoccaggio e vendite dei prodotti per ciascun supermercato. Ogni scontrino specifica i codici prodotti venduti, quantità, prezzo unitario, sconti, modalità di pagamento e data. Dopo la chiusura giornaliera dei supermercati vengono selezionate le registrazioni “testata-scontrino” “dettaglio-scontrino” del giorno e copiate nella *staging area*. I dati vengono filtrati, puliti e memorizzati un *operational data store*. Tramite operazioni di select e join si ottiene una nuova tabella “registrazione riepilogativa” che contiene i punti vendita, l’articolo venduto, la data, la quantità totale di vendita del prodotto nel punto vendita, l’importo totale delle vendite del prodotto nel punto vendita, il numero degli scontrini emessi del prodotto nel punto vendita.

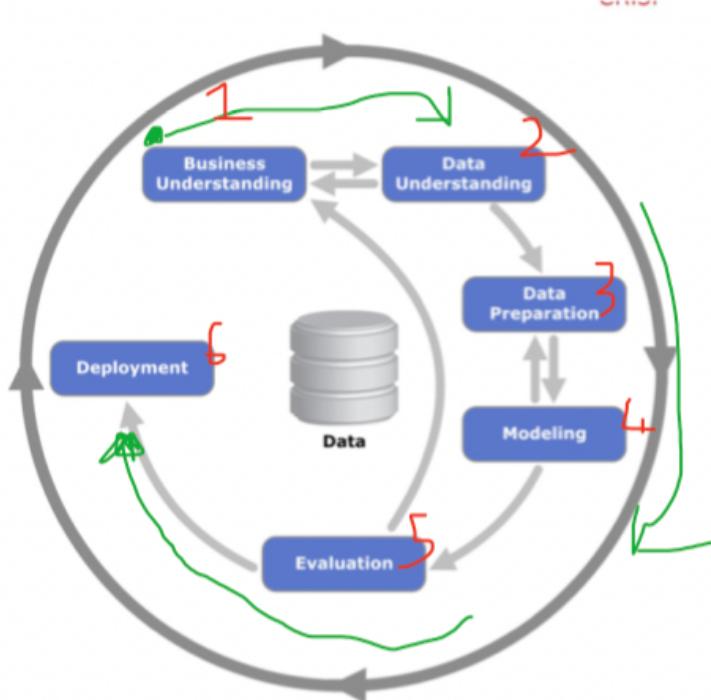
Il **cubo di dati** permette un’analisi su 3 dimensioni, nel caso generale di più dimensioni si ottiene un ipercubo, applicando all’esempio un cubo avremmo sui tre lati: le date, il negozio ed il prodotto -> ogni “tassello del cubo” indica la quantità di pezzi venduto, il prezzo di vendita e di acquisto in un determinato giorno, di un determinato prodotto in un determinato negozio.



La business intelligence si basa sull’informazione per generare un’analisi descrittiva (utilizzo dell’intuito), l’**analisi dei dati (data analytics)** si occupa di metodi più difficili -> analisi diagnostica, predittiva (quale sarà la prossima azione migliore per migliorare il business?) e prescrittiva.

CRISP-DM

Cross Industry Standard Process for Data Mining



Metodologia generale per affrontare problemi di data mining, proviene da progetto europeo alla fine del 900. È diventato uno standard aperto (non viene più aggiornato). Per affrontare l'analisi dei dati è importante eseguire il ciclo che inizia dal comprendere cosa serve al business (business understanding) e finisce al deployment.

- 1) Quali sono i bisogni del business
- 2) Di che dati abbiamo/ necessitiamo
- 3) Come organizziamo i dati per il modello?
- 4) Quale tecniche di modellazione bisogna applicare?
- 5) Quali modelli si applicano meglio agli obiettivi del business?
- 6) Come gli stakeholders possono accedere ai risultati?

Con il termine **big data** si intendono basi di dati che hanno tre caratteristiche peculiari (3+1 V):

Volume: ingenti quantitativi di dataset non gestibili con i database tradizionali

Velocity: dati che affluiscono e necessitano di essere processati a ritmi sostenuti o in tempo reale

Variety: dati di diversa natura e non strutturati come testi, audio, video, flussi di click etc.

Veracity: veridicità dei dati

Il monitoraggio dei dati dei social media genera big data: analisi dei tag, dei commenti associati ai contenuti, relazioni tra utenti, immagini, NLP per sentiment analysis. Alcune piattaforme per Big Data sono: Microsoft Azure HDInsight, Oracle Big Data SQL, HP Vertica etc.

Mapreduce (Google) è un modello di programmazione parallelizzabile su cluster di HW commerciale, *Map* è una funzione che elabora una coppia chiave/valore per generare un insieme di coppie chiave/valore intermedie (da una stringa in input emette la lunghezza della parola come chiave e la parola stessa come valore); *Reduce* è una funzione che combina tutti i valori intermedi associati con la stessa chiave intermedia (conta il numero di elementi nella lista precedente ed emette la chiave con la dimensione della lista).

Apache Hadoop è un framework ispirato a MapReduce, con grande scalabilità e tolleranza ai guasti.

Un **cruscotto aziendale** è uno strumento che consente una visione di sintesi delle diverse aree aziendali. Fornisce una visione immediata dell'andamento di diversi settori, tenendo sotto controllo gli indicatori più importanti che caratterizzano il funzionamento di una azienda. Contengono gli *indicatori (KPI)* che sono valori di sintesi per valutare il funzionamento dell'azienda e dei diversi settori, sono valutati tramite i *range* che rappresentano graficamente con colori il loro andamento rispetto all'obiettivo prefissato. I cruscotti permettono una navigazione drill down con diversi livelli di approfondimento, e possono essere organizzati in mappe per aree tematiche e settori aziendali (produzione, commerciale, risorse umane, logistica etc.) per migliorarne la leggibilità.

Capitolo 7 – Aziende ed internet

L'azienda online è composta dall' **intranet aziendale**, prerequisito per la realizzazione di un sistema informatico integrato e la creazione di un modello di integrazione applicativa. L'**extranet**, rete privata virtuale sicura, basata su tecnologia IP per abilitare interazioni applicative dirette con fornitori partner, terze parti e clienti business ed infine l'**internet**, canale preferenziale di interazione con gli utenti consumer, che richiede ai sistemi aziendali la fornitura di informazioni in maniera immediata ed accurata.

Internet ha modificato profondamente tutti i paradigmi degli affari e dei commerci, le principali novità sono:

- *Annullo delle distanze*: globalizzazione dei mercati, gli intermediari la cui attività non crea valore entrano in crisi.
- *Trasparenza*: gli acquirenti sono più informati, i costi della trasparenza diminuiscono (politiche e-Gov).
- *Struttura a rete*: emergono le imprese con struttura a rete, da modelli organizzativi locali basati sulla vicinanza geografica a modelli organizzativi basati sulla rete.
- *Virtualizzazione*: nuove catene del valore diventano possibili, si aprono opportunità per nuove forme e figure economiche che aggiungono valore

- *Creatività*: nuovi modi di organizzare business esistenti, nuove opportunità di business.
- *Velocità*: criticità del tempo di risposta del mercato
- *Evoluzione*: difficoltà a sostenere il vantaggio competitivo nel tempo.

L'**E-business** consente la facilitazione di funzioni, processi e specifiche strategie aziendali utilizzando tecnologie web/internet per la condivisione e l'integrazione di flussi informativi ed applicazioni, un modello di riferimento a 4 livelli:

- Modello di business: *business-to-business(B2B)* tutti i trasferimenti di un'azienda e i suoi fornitori o altre aziende (scambio di informazioni strutturate tra aziende, sistema efficiente per risposte in tempi brevi con numero di utenti noto a priori); *business-to-consumer* (B2C) servizi di vendita al dettaglio di beni vari (sistema deve garantire scalabilità in quanto il numero di utenti non è noto a priori); *consumer-to-consumer*, meccanismi di asta su rete; *government-to-business*, servizi verso le aziende ,informazioni, pagamento di tasse; *government-to-Citizens*: informazioni e servizi verso i cittadini.
- Modello di comportamento del cliente: come il cliente naviga all'interno del sito.
- Modello delle infrastrutture tecnologiche: analisi delle prestazioni dei sistemi di elaborazione e comunicazione utilizzati, previsione del grado di soddisfazione rispetto alle esigenze.

Alcuni modelli di E-business sono:

- *Comunità virtuale*: membri ed utenti finali giocano il ruolo di operatori attivi o clienti in un'alleanza che non possiede controllo gerarchico. (sviluppo open source come Linux)
- *HUB*: sito gestito che attraverso un processo di gestione genera valore mediante l'integrazione.
- *E-MALL* aggregazione di vendori che costituiscono un unico distributore virtuale, meccanismi di vendita in rete mediante asta.

Il mercato odierno è caratterizzato dalla vendita di beni “immateriali”, canzoni, film, video, software e tutto ciò che è trasportabile attraverso la rete. Alcuni tipi di siti legati all'e-commerce sono i siti istituzionali di aziende, E-SHOP B2C o B2B etc.

Le funzionalità minime di un E-shop sono la presenza di un catalogo di prodotti, una funzione di acquisto, una raccolta di dati utente (ovvero la registrazione), un sistema di tracciatura dell'utente e la presenza di servizi aggiuntivi (come lista della spesa, notifiche via e-mail etc.)

iTunes è un esempio di vendita di beni “immateriali”, è un E-shop per la vendita di musica digitale, video musicali e film gestito dalla Apple Inc, comprende più di 6

milioni di canzoni, le canzoni sono codificate nel formato Dolby Advanced Audio Codin (AAC) a 128 kb/s, le canzoni sono legate ai prodotti hardware Apple.

Amazon è un esempio di E-shop di prodotti “facilmente trasportabili”, iniziò come libreria online, oggi vende praticamente di tutto. L’azienda ha una sua propria catena distributiva basata su magazzini dislocati sul territorio, il trasporto è demandato a corrieri internazionali con tracciamento delle spedizioni.

Esprinet è un’azienda italiana (presente anche in Spagna), E-Shop B2B per la vendita di prodotti informatici a rivenditori e aziende afferenti al settore ICT.

Alcuni fattori rilevanti per un E-Commerce sono: la *percezione* del valore per il cliente, l'*usabilità* e la *scalabilità* del sito, la *qualità* del servizio offerto, la *protezione* dei dati rispetto ad attacchi e la *robustezza* rispetto ai guasti, la *forza* del brand ed infine la *posizione* sui motori di ricerca.

Un caso: Google

Google è attualmente il motore di ricerca più popolare e utilizzato in INTERNET, la tecnologia GOOGLE si basa su algoritmi di ricerca molto sofisticati e su una metodologia per individuare l’importanza dei documenti (*page ranking*).

L’architettura è distribuita ed altamente complessa, include sistemi di memoria che ospitano enormi database e server farm distribuite che forniscono la potenza di calcolo. I motori di ricerca su internet iniziarono ad essere sviluppati nei primi anni 90 in diverse università (Archie, Veronica, WWW Wanderer (MIT)), per favorire la condivisione di informazione tra i ricercatori. La ricerca su internet diventa l’unico modo efficace di utilizzare il WWW, quasi tutti i motori di ricerca nascono nelle università ad eccezione di Altavista, Google è il prodotto di due studenti di dottorato a Stanford (Page e Brin) che avevano sviluppato un sistema di ricerca documenti all’interno dell’Università. La ricerca su WEB è un contenitore per vendere pubblicità, il vantaggio di Google è quello di offrire un servizio di ricerca più accurato ed efficiente di altri motori. Lo scopo di Google era quello di organizzare il mondo di Internet per rendere le informazioni accessibili, nel 2001 Google identificò il suo core business nella pubblicità online, che compare sia sulle pagine dei risultati del motore di ricerca sia sui siti web partner che mostrano la pubblicità fornita da Google.

Google ha creato uno schema di pagamento basato sul “cost-per-click” tale che gli inserzionisti pagano un contributo fisso ed una ulteriore quota che dipende dal numero di volte che gli utenti fanno riferimento al sito pubblicizzato.

I diversi tipi di pubblicità presenti su internet si possono classificare in tre categorie:

- *Banner Ads*: piccoli spazi standardizzati da inserire all’interno di una pagina, il proprietario di un sito destina questi elementi ad una società esterna che carica i messaggi pubblicitari. La società fa da intermediaria tra chi offre lo spazio pubblicitario e chi vuole pubblicare la propria pubblicità.

- *Context Linked Ads*: link pubblicitari collegati al contesto della pagina nella quale sono pubblicati, *Google AdSense* sceglie quali context link aggiungere all'interno di una pagina.
- *Search Linked Ads*: link pubblicitari presenti direttamente all'interno delle pagine dei motori di ricerca, le pubblicità sono legate ai termini di ricerca utilizzati dall'utente; per Google questo tipo di pubblicità viene gestito dalla *Google AdWords* (cioè aggiungi parole).

Lo scopo di Google è vendere spazi pubblicitari presenti sulle pagine di ricerca facendo in modo che le pubblicità siano quanto più attinenti al tema della query, deve fornire la miglior vetrina possibile all'utente che compie una ricerca per invogliarlo ad acquistare o visitare la pagina web. Chi si occupa di realizzare il messaggio pubblicitario si deve concentrare sul contenuto in modo che sia conciso ma accattivante, mentre Google si occupa di come e quando deve essere visualizzata la pubblicità.

Se una pubblicità non raggiunge una soglia minima di click, fissata a priori, allora sarà disabilità (ovvero non più visualizzata); il rivenditore può decidere di fare visualizzare in modo casuale a tiro tutti i messaggi pubblicitari che ha preparato e Google mostrerà più frequentemente quello che genera più click.

Google classifica il successo delle pubblicità attraverso il *CTR (click through rate)*, ovvero la percentuale di click effettuati da visitatori su un annuncio o un banner pubblicitario in relazione al numero di visualizzazioni di una pagina web.

Per stabilire il prezzo di vendita delle posizioni migliori la maggior parte dei motori di ricerca utilizza il metodo dell'asta all'inglese (miglior offerente si aggiudica la posizione al prezzo da lui offerto), Google invece utilizza il metodo *Vickrey Auction* (utilizzato anche da Ebay), in cui il prezzo finale è stabilito non in base all'offerta più alta ma in base alla seconda offerta maggiore. Tutte le offerte vengono raccolte all'inizio per evitare meccanismi di rialzo speculativi, gli acquirenti devono essere in grado di stimare la propria offerta massima -> meccanismo vantaggioso per gli acquirenti che devono pagare il minimo prezzo necessario per mantenere la posizione. *AdWords Discounter* è il meccanismo che si occupa di gestire le aste, le aziende infatti non devono preoccuparsi di seguire l'andamento dell'asta ma devono soltanto fissare la massima offerta che sono disposte a pagare per quella posizione. *AdWords* offre diverse strategie di offerte adatte per i diversi tipi di campagne pubblicitarie: *cost-per-click-bidding* (per spingere i clienti al proprio sito), *cost-per-impression binding* (per assicurarsi che i clienti vedono i messaggi dell'inserzionista), *cost-per-acquisition bidding* (acquisti o registrazioni utente).

Le **entrate** secondo il modello business di Google sono date dalla seguente espressione matematica:

$$\text{Entrate} = \frac{\text{Utenti}}{\text{Utente}} * \frac{\text{Interrogazioni}}{\text{Interrogazione}} * \frac{\text{Annunci}}{\text{Annuncio}} * \frac{\text{Click}}{\text{Click}} * \frac{\text{Ricavo}}{\text{Click}}$$

Quantità – Qualità - Prezzo

In media una ricerca su Google richiede la lettura di centinaia di Mbytes e l'esecuzione di miliardi di istruzioni, Google dispone di diversi data center distribuiti geograficamente ai quali le richieste vengono trasmesse sulla base della vicinanza geografica. Ogni data center contiene diverse copie dell'intero WEB in modo da poter servire con grande affidabilità richieste diverse in parallelo.

Un **inverted index** è una struttura che associa parole alla loro posizione all'interno di un documento e consente ricerche a testo pieno, esistono due varianti:

- *Record level inverted index*: contiene solo la lista dei documenti nella quale la parola compare.
- *Word level inverted index*: contiene anche la posizione della parola nel testo e serve per trovare frasi all'interno di un testo.

ESEMPIO (da Wikipedia)

Dati i testi $T_0 = \text{"it is what it is"}$, $T_1 = \text{"what is it"}$ e $T_2 = \text{"it is a banana"}$, si hanno i seguenti *inverted file index* (dove gli interi fanno riferimento al numero d'ordine del testo) :

"a": {2} "banana": {2} "is": {0, 1, 2} "it": {0, 1, 2} "what": {0, 1}

Una ricerca delle parole "what", "is" e "it" da il seguente risultato

$$\{0, 1\} \cap \{0, 1, 2\} \cap \{0, 1, 2\} = \{0, 1\}$$

Il **PageRank** è uno dei metodi che Google utilizza per definire l'importanza di una pagina WEB, è un valore numerico calcolato per ogni WEB sulla base dei dati immagazzinati nei siti di Google.

Assumiamo che la pagina A abbia $T_1 \dots T_n$ pagine che puntano ad essa (ovvero la citano), il parametro d è un fattore di smorzamento (tra 0 ed 1, normalmente pari a 0.85), $C(A)$ è il numero di link uscenti da A (le pagine che cita). Il pageRank di A è dato da:

$$PR(A) = \frac{1-d}{N} + d \left(\frac{PR(T_1)}{C(T_1)} + \dots + \frac{PR(T_N)}{C(T_N)} \right)$$

Quindi: $PR(T_N)$ è il pagerank di ogni singola pagina, $C(T_N)$ è il numero di link che sono contenuti in una pagina, $\frac{PR(T_n)}{C(T_n)}$ è la *frazione di fiducia* di una pagina verso la pagina A.

PageRank può essere pensato come un modello di un “navigatore casuale” che a partire da una pagina casuale continua a fare click a caso sui link della pagina, il valore di d è associato alla probabilità che il navigatore ricominci a caso da una nuova pagina. Il valore PR(A) sarà alto per una pagina se vi sono molte pagine che puntano ad essa oppure anche solo poche pagine ma con un PageRank elevato.

Un **social network** consiste in un gruppo di individui qualsiasi connessi tra loro da diversi legami sociali, la versione di internet delle reti sociali è una delle forme più evolute di comunicazione in rete.:

Social media è un termine generico che indica tecnologie e pratiche online che le persone adottano per condividere contenuti testuali, immagini, video ed audio. Si può definire social network un social media specifico per le relazioni sociali. Un social network è caratterizzato da un *bacino d'utenza globale, accessibilità* in quanto i social media sono disponibili da ogni individuo a un costo contenuto o gratuitamente, *fruibilità, velocità*: i social media scambiano informazioni in tempi brevi, *permanenza*: i social media possono essere cambiati quasi istantaneamente mediante commenti e modifiche, *basso costo* rispetto ai media tradizionali.

È possibile distinguere diversi tipi di social media:

Social media generalisti: sono la fusione di community, blog, sono aperti al grande pubblico, tra i più famosi in Italia abbiamo Facebook e Google.

Social network specifici per categoria di contenuto: sono legati alla condivisione di una particolare categoria di contenuto, aperti al grande pubblico ad esempio Youtube, Twitch e flickr.

Social network professionali: sono legati alla condivisione di informazioni su tematiche professionali e di domanda/offerta di lavoro, ad esempio Linkedin

Microblogging: sono un'evoluzione dei forum, ogni utente ha la sua bacheca dove pone messaggi di lunghezza limitata, il più famoso è Twitter.

Piattaforme di pubblicazione permettono la facile pubblicazione di contenuti, possono essere organizzate o libere (esempi sono Wikipedia, Wordpress)

Piattaforme di condivisione: permettono la facile condivisione di contenuti, possono essere organizzate o liberi. Alcuni esempi sono google drive, Icloud, Dropbox, Mega etc.

Storia dei social network: si inizia con i *newsgroup*, spazi virtuali creati su una rete di server interconnessi (Usenet) per discutere di un argomento ben determinato, nel 2001 si passa ai *blog*, sito web gestito da una persona (o una struttura), in cui l'autore scrive periodicamente come in una sorta di diario online. Successivamente si passò alle *virtual community*, persone che condividono pratiche, attività, interessi lavorativi attraverso il web: avviene il trasferimento del concetto di comunità del mondo reale a quello della rete. Nel 2005 avviene l'avvento del web 2.0, la rete da quasi monodirezionale diventa bidirezionale: gli utenti accedono e pubblicano contenuti (blog, wiki, forum, community), avvento dei social media ottenuti attraverso opportune tecniche di programmazione afferenti al paradigma del web dinamico.

I contenuti principali di un social network sono:

- *Contenuto primario*: ovvero il testo, l'immagine, il video, l'audio etc.
- *Tag*: parole chiave che accompagnano il testo
- *Link*: indirizzi di altre risorse in rete presenti o associati al testo
- *Commenti*: risposte o indicazioni di gradimento associati al contenuto pubblicati da altri utenti

- *Thread*: flusso di commenti relativi ad uno stesso contenuto iniziale
- *Discussione*: thread particolare appartenente ad un gruppo.

L'*utente* è caratterizzato da nome, dati, foto etc. Ha un suo spazio specifico dei contenuti e può interagire con i contenuti degli altri ed inviare o ricevere messaggi diretti. I *gruppi* nei social network possono essere tematici o no.

I social media possono essere utilizzati in un piano di business, una volta identificati: il target (e quali social frequenta), l'obiettivo da raggiungere, la spesa da investire e le modalità di azione (*strategia monocanale*, scegliendo un social media specifico, oppure *strategia multicanale*, scegliendo una combinazione di social media ed un sito/portale web). Esempio celebre è il caso *Dave Carroll* -> la chitarra del cantante viene danneggiata durante viaggio tramite United Airlines, le sue richieste di risarcimento vengono ignorate. Carroll realizza un video musicale sulla sua vicenda e lo pubblica su youtube, una volta diventato virale scrive un libro a riguardo e la Airlines United subisce una perdita di circa 200 milioni di incassi.

Un social network può offrire *servizi freemium*: una versione base gratuita con dei limiti ed una versione premium a pagamento. Per i *servizi free* il business del fornitore di servizio consiste nei dati che l'*utente* cede all'azienda.

Bisogna ricordare però che siamo noi utenti che scegliamo cosa pubblicare in rete e dovremmo sapere cosa c'è dietro e saper sopesare ogni azione che compiamo.

ICT e-Business: presente e prospettive

Lo scopo primario dei **sistemi informatici** è fare business, più o meno direttamente (producendo direttamente reddito o svolgendo compiti entro i sistemi informativi). L'azienda necessita un'interconnessione totale entro l'azienda per garantire la disponibilità delle informazioni fra le sezioni, una flessibilità ed economicità delle strutture IT.

Dal 1995 nelle ICT si è assistito a tre grandi migrazioni strutturali avvenute in rapida successione: e-commerce (che ha modificato profondamente le modalità di interazione fra impresa e clienti), e-business (ha avuto un impatto simile su fornitori e dipendenti), m-business indurrà cambiamenti più profondi perché onnipresente. Un altro cambiamento è dato dall'introduzione di vendita di beni immateriali e dalla delocalizzazione della produzione software, dei centri di calcolo e dei call center. L'azienda deve quindi essere rapida nella reazione ai mutamenti e nuove esigenze imposte dal mercato globale, e quindi: avere un uso ottimale dell'ICT, organizzazione per processi, politiche di gestione di qualità ridurre carico e costi interni, rapidità di reazione e proattività. Inoltre, è utile migliorare i canali di comunicazione interni, lo scambio di idee al proprio interno e poter raccogliere contributi creativi di tutti i propri collaboratori ma anche dei propri clienti -> azienda social. Il trend attuale è dato dal **paradigma SMAC**:

Social media

Mobility
Analytics
Cloud Computing
(Internet of things)

Capitolo 8 – Gestione dei sistemi IT

Sistema informativo ed obiettivi di business: IT Governance

All'interno di un'azienda l'IT viene vista con una percezione negativa, quando in realtà è una risorsa importante per l'impresa. Il **governo d'impresa** definisce l'insieme di regole, di ogni livello, che disciplinano la gestione e il controllo della società.

La **governance** deve garantire che gli obiettivi dell'organizzazione siano ottenuti attraverso la valutazione dei bisogni, delle condizioni e delle opzioni di tutti gli stakeholder, impostando le linee guida attraverso la prioritizzazione e le decisioni e monitorando le performance e la compliance rispetto agli obiettivi prestabiliti -> *evaluate-direct-monitor*.

Il **management** deve pianificare, definire, eseguire e controllare le attività in allineamento con le direzioni impostate dal gruppo di lavoro che imposta la governance per ottenere gli obiettivi dell'organizzazione. Lo standard **COBIT** (Control objectives for information and related technology) nasce negli anni 90 (ultima versione COBIT 2019), è un quadro di riferimento per la governance ed il management delle informazioni e della tecnologia aziendale. Per *enterprise I&T* si intende tutta la tecnologia e l'elaborazione delle informazioni dell'impresa per raggiungere i propri obiettivi, indipendentemente dal luogo in cui ciò accade in azienda e non si limita al reparto IT (che è compreso). Mette insieme 5 *principi fondamentali* per permettere all'azienda o all'organizzazione di costruire una effettiva IT governance ed un effettivo IT management attraverso l'uso pragmatico di 7 *elementi di abilitazione* che possono ottimizzare gli investimenti in tecnologie ed informazione per usarli a beneficio degli stakeholder.

I 5 principi sono:

1. Andare incontro ai bisogni degli stakeholder -> creazione di valore
2. Coprire l'azienda in modo end-to-end: tutte le funzioni ed i processi aziendali e non solo quelli IT
3. Applicare un singolo framework integrato
4. Rendere possibile un approccio olistico
5. Separare la governance dal management

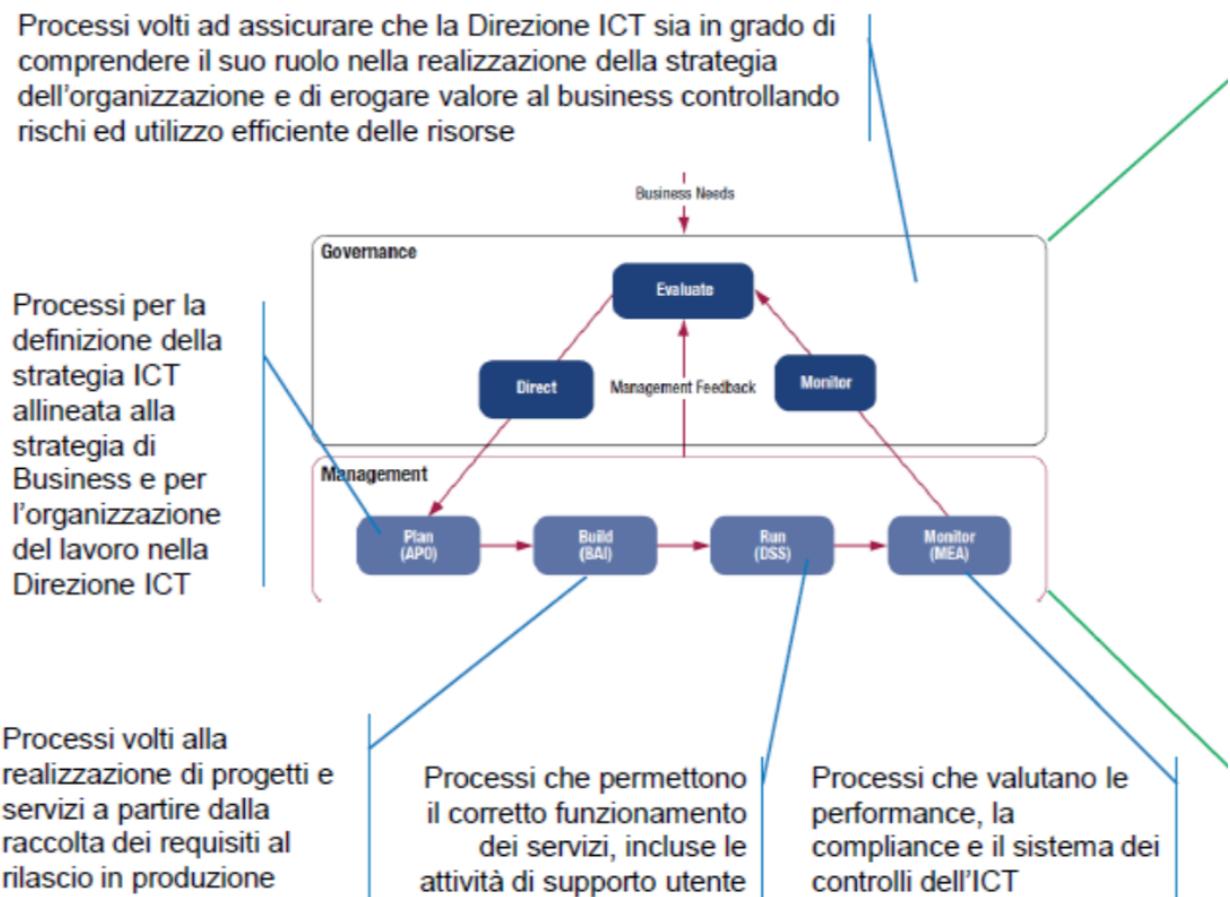
I 7 enabler sono:

1. Principi, politiche e framework
2. I processi

3. Le strutture organizzative
4. Cultura, etica e conoscenza
5. L'informazione
6. Servizi, infrastrutture ed applicazioni
7. Le persone, le loro skill e le competenze

Cosa è / non è un COBIT: è un framework per la governance ma non per organizzare i sistemi di Business, definisce i componenti da costruire e sostenere in un governance system ma non prende o suggerisce nessuna decisione riguardo l'IT.

Processi volti ad assicurare che la Direzione ICT sia in grado di comprendere il suo ruolo nella realizzazione della strategia dell'organizzazione e di erogare valore al business controllando rischi ed utilizzo efficiente delle risorse



Il **ROI** (return of investment) in ICT può essere espresso mediante una definizione quantitativa o qualitativa dei benefici, i limiti del ROI sono dati dall'esclusione di costi difficili da quantificare, dalla penalizzazione degli investimenti al lungo termine ed è un indice troppo semplificativo e non integrabile con la pianificazione. Per *valutare i benefici* bisogna qualificare tutti i potenziali benefici, sia quelli tangibili che no, definire il ROI sui valori monetizzati ed integrarlo con valori quantificati ma non monetizzati; infine bisogna completare l'operazione con considerazioni strategiche e organizzative.

Per quanto riguarda la qualificazione dei benefici alcune voci sono:

l'automatizzazione dei benefici, la riduzione dei costi, lo spostamento dei costi, miglioramento delle prestazioni, riduzione del rischio.

Per quantificare i benefici le voci monetizzabili sono: riduzione del personale, del costo di struttura, di altri fattori produttivi, del magazzino e l'eliminazione dei costi tecnologici di sistemi obsoleti.

Per i benefici non monetizzabili si potrebbe pensare alla riduzione dei tempi di servizio, dei tempi di evasione ordini e l'implementazione di una maggiore rapidità di esecuzione di operazioni.

Il **TCO** (total cost of Ownership) comprende I costi di acquisto/sviluppo sia hardware che software, ma anche i costi di attivazione, assistenza e manutenzione (e possibile evoluzione). Bisogna analizzare accuratamente i *punti critici dei propri sistemi*: ad esempio, i sistemi operativi non sono sempre sufficientemente robusti rispetto a condizioni operative non frequenti, le macchine hanno parti meccaniche soggette ad usura e la componentistica elettronica può presentare dei problemi. Altri problemi da considerare sono la *complessità lato software* (vecchi e nuovi bug, modularizzazione, tempi di comprensione da parte dell'utente lunghi) e il *tempo di fermo macchina (downtime)*.

La formula per misurare il costo del fermo macchina è:

$$\text{costo fermo macchina} = O * \left(T * \frac{P}{100} \right) * (C + F)$$

Con O pari al numero di operatori, T il tempo di fermo macchina, P la percentuale di inattività del fermo macchina, C il costo di una persona, F il reddito prodotto da una persona.

Per valutare i costi annui della spesa informatica è possibile procedere mediante un'*analisi aggregata* (livello ed incidenza della spesa informatica) -> entità assoluta della spesa oppure analisi incrociata (dimensione spesa/dimensione impresa).

Mediante un'*analisi disaggregata* (struttura della spesa informatica) -> per tipo di risorsa, funzione del reparto oppure per prodotto.

Il *valore assoluto* della spesa deriva da dati puntuali e relative voci identificative, dalle serie storiche (ovvero curve di spesa) e dall'associazione con le acquisizioni di strumenti ICT.

Per il *valore incrociato* si hanno due approcci: incrocio con volumi produttivi (a valore, ad esempio il fatturato, oppure a quantità, ad esempio unità prodotta) incrocio con monte risorse (a valore, ad esempio costo delle persone, o a quantità numero dei dipendenti).

Le politiche di gestione

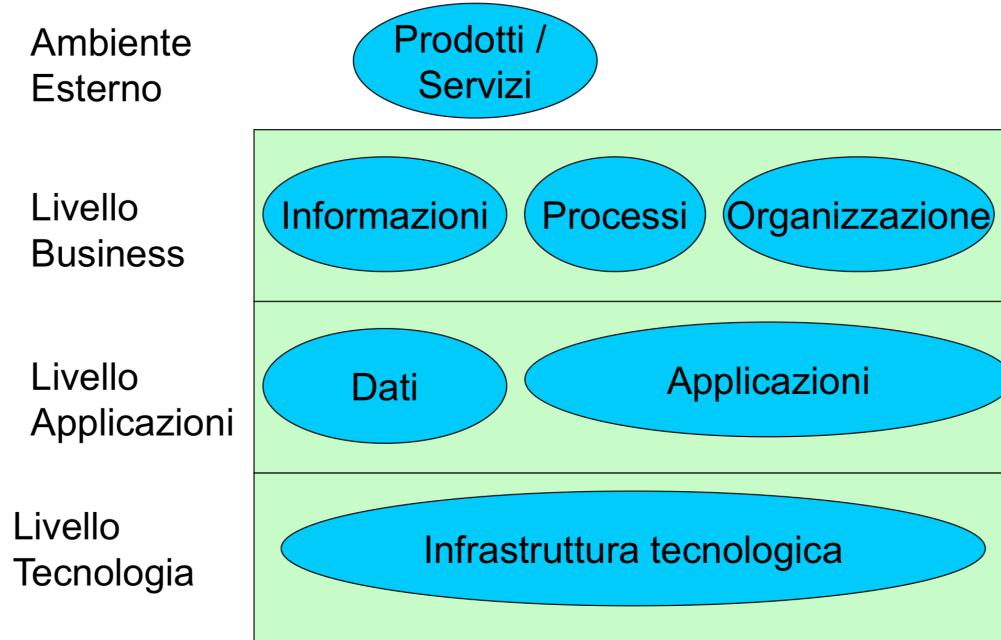
La gestione di un'azienda riguarda diversi fattori -> gestione operativa, gestione delle risorse, gestione della configurazione, gestione dei problemi (procedure di

salvataggio e piani di disaster Recovery). Suddividiamo 3 livelli di politiche di gestione:

- *Politiche generali*: una policy definisce una posizione di alto livello su un argomento, non definisce come fare qualcosa e non definisce i dettagli e devono essere concordate con la direzione generale. (Es. information security policy, disaster recovery policy etc.)
- *Standard*: stabilisce come qualcosa dovrebbe essere configurata, non specificano come qualcosa viene svolto nei dettagli e dovrebbero cambiare seguendo processi e tecnologia (standard di configurazione di macchine unix o windows, di configurazione di un database e di un sito web etc.)
- *Procedure*: provvedono istruzioni dettagliate su come implementare le politiche, definiscono anche chi è responsabile per ogni azione passo dopo passo e cambiano di frequente e dovrebbero essere aggiornate regolarmente attraverso un processo standardizzato.

Oltre al **COBIT**, altri standard sono TOGAF, ITIL, ISO 20000, 27000, 25000, 385000, 42010.

Il **TOGAF/ARCHIMATE** è un framework che prevede un approccio globale alla progettazione, pianificazione, attuazione, e la governance di un'architettura all'interno di un'impresa; l'architettura è in genere modellata a quattro livelli o domini: business, dati, applicazioni, tecnologia.



L'**ITIL** è l'acronimo di Information Technology Infrastructure Library, è un insieme di linee guida nella gestione dei servizi IT e si basa sulla sequenza di 5 macro-processi fondamentali:

- **Service Strategy**: Il punto centrale e di origine del ciclo di vita del servizio ITIL, fornisce indicazioni sull'aiutare le organizzazioni IT a migliorare e a svilupparsi a lungo termine, Service Strategy si basa in gran parte su un approccio orientato al mercato. La fase del ciclo di vita del SS è definita dal:

- *Service Portfolio Management*: garantire che le offerte di servizi offerti dal fornitore siano definite e soddisfino i requisiti dei clienti. Il **service Portfolio** è un database che contiene tutte le informazioni su tutti i servizi (presenti, passati e futuri), si divide in tre parti: *service catalogue* che contiene tutte le informazioni esatte su tutti i servizi in esercizio e su quelli che sono pronti per esserlo (Business service Catalogue -> vista cliente, Technical Service Catalogue -> rafforza il business catalogue ma non forma parte della vista cliente). La stratificazione dei catalogue si riporta su quella dei tre livelli di TOGAF, conoscere e controllare appieno un servizio significa quindi conoscere la successione dei suoi configuration item attraverso gli strati di TOGAF e poterli controllare e manutenere tutti.
 - *Financial Management*: garantire che l'infrastruttura IT sia ottenuta al prezzo più efficace e calcolare il costo della fornitura dei servizi IT in modo che un'organizzazione possa comprendere i costi dei suoi servizi IT.
 - *Business Relationship Management*: un approccio formale alla comprensione, alla definizione e al supporto delle attività aziendali relative al business networking
 - *Demand Management*: metodologia di pianificazione utilizzata per prevedere, pianificare e gestire la richiesta di prodotti e servizi
 - *Strategy Management*: valutare le offerte, le capacità, i concorrenti del fornitore di servizi e gli attuali e potenziali spazi di mercato al fine di sviluppare una strategia per servire i clienti.
- **Service Design**: trasforma la strategia di un servizio in un piano per la realizzazione degli obiettivi aziendali. I processi presenti in questo volume sono:
- *Design Coordination* mira a coordinare tutte le attività, i processi e le risorse di progettazione dei servizi.
 - *Service Catalogue Management* mantiene e produce il catalogo dei servizi e garantisce che contenga dettagli accurati, dipendenze e interfacce di tutti i servizi resi disponibili ai clienti.
 - *Service Level Management* prevede l'identificazione, il monitoraggio e la revisione continua dei livelli dei servizi IT specificati negli SLA
 - *Supplier Management* gestisce i servizi forniti dai fornitori cercando di ottenere un'elevata qualità dei servizi in base al loro valore monetario.
 - *Availability Management* consente alle organizzazioni di sostenere la disponibilità del servizio IT al fine di supportare il business a costi giustificabili.

- *Capacity Management* supporta la fornitura ottimale ed economica dei servizi IT, aiutando le organizzazioni ad abbinare le proprie risorse IT alle esigenze aziendali.
 - *IT Service Continuity Management* copre i processi mediante i quali i piani vengono implementati e gestiti per garantire che i servizi IT possano riprendersi e continuare anche dopo che si è verificato un incidente grave.
 - *Information Security Management* descrive l'adattamento strutturato della sicurezza delle informazioni nell'organizzazione di gestione.
- ***Service Transition:*** sviluppa e migliora le capacità di introdurre nuovi servizi negli ambienti supportati. I processi presenti in questo volume sono:
- *Change Management*, mira a garantire che vengano utilizzati metodi e procedure standardizzati per gestire in modo efficiente tutte le modifiche.
 - *Service Asset and Configuration Management* è principalmente incentrata sulla gestione delle informazioni necessari per fornire un servizio IT, incluse le loro relazioni.
 - *Release and Deployment Management* viene utilizzata dal team di migrazione del software per la distribuzione automatica e indipendente dalla piattaforma di software e hardware.
 - *Il Knowledge Management* controlla che le informazioni siano corrette e disponibili a chi deve prendere delle decisioni.
- ***Service Operation:*** gestisce i servizi negli ambienti supportati. Si basa su funzioni e processi, per quanto riguarda le funzioni abbiamo il *service desk*, *technical management*, *l'application management* ed infine *l'IT operation management*.
- Per i processi invece: *event management*, *incident management*, *access management*, *problem management* ed infine il *request fulfillment*. Un *incidente* è un'interruzione non programmata o una riduzione della qualità imprevista di un servizio IT, anche la configurazione sbagliata di *Configuration Item* è un incidente. Un *problema* è la causa di uno o più incidenti, la sua causa non è conosciuta nel momento in cui viene registrato.
- ***Continual Service Improvement:*** realizza servizi incrementali e miglioramenti su larga scala. Si basa sul *seven-step improvement process*.

L'**ISO 20000** è il primo standard internazionale per la gestione dei servizi IT, composto in due sezioni:

- ISO 20000-1: promuovere l'adozione di un approccio a processo integrato per mettere effettivamente in opera servizi gestiti per venire incontro alle esigenze del business e dei clienti.
- ISO 20000-2: Definisce un insieme di best practice per ogni sezione, fortemente basato su ITIL ma con riferimenti anche ad altri framework

L'**ISO 42010** riguarda lo standard delle architetture per il software, per i sistemi e per le aziende; definisce quattro conformità allo standard:

- Descrizione dell'architettura
- Punti di vista dell'architettura
- Framework per l'architettura
- Linguaggi di descrizione per l'architettura (come BPMN ed UML)

Profili professionali nell'IT

Gli ambienti in cui l'ICT è il core business sono le software house, i rivenditori di hardware e software, i fornitori di servizi via internet, fornitori di cloud e di servizi di elaborazione dati. Ci sono ambienti in cui l'ICT supporta il core business: le banche, aziende, infrastrutture, sanità, P.A., educazione etc.

I dipartimenti IT si suddividono in:

Sezione dell'azienda, che si occupa delle specifiche tecniche dell'ICT aziendale

EDP interno per l'analisi ed i test o la produzione

Fornitore IT esterno per l'analisi, lo sviluppo e i test dell'ICT aziendale.

Un errore nelle specifiche aumenta il proprio impatto nelle fasi successive.

Le categorie di progetti IT in base alla loro complessità troviamo: realizzazioni di programmi custom, realizzazione di programmi a partire da semi-lavorati, installazione e customizzazioni di programmi esistenti ed infine sistemi infrastrutturali.

I *ruoli tradizionali* per i progetti di sviluppo SW lato cliente (spesso non hanno competenze informatiche) sono:

- *Cliente*: può essere l'azienda stessa che compra il progetto, conosce le necessità per cui il progetto nasce.
- *Acquirente*: funzionario dell'azienda cliente che compie le trattative commerciali, spesso fa parte dell'ufficio acquisti e quasi sempre non conosce le esigenze di dettaglio degli utenti finale
- *Utente*: utilizzatore del sistema ICT.

I *ruoli tradizionali* per i progetti di sviluppo SW lato fornitore sono:

- *Analista funzionale*: ha esperienza di analisi di processo, scrive le specifiche funzionali di dettaglio (user experience ed user interface specialist sono gli analisti funzionali della UI).

- *Analista tecnico*: svolge la combinazione dei lavori di progettista di alto livello e progettista di dettaglio nei progetti più piccoli.
- *Progettista di alto livello*: chiamato anche software architect, ha grande esperienza informatica e conosce il tool/linguaggio/metodologia di sviluppo, il suo compito è quello di tradurre le specifiche funzionali in un'architettura software ben definita.
- *Progettista di dettaglio*: ha buona esperienza informatica, partendo dall'architettura definisce il dettaglio di tutte le componenti. Produce una serie di specifiche per ogni singolo componente software
- *Programmatore*: in base alle specifiche ricevute, scrive e verifica il codice. Provvede ai test intermedi e sotto la guida del capo progetto provvede all'integrazione.
- *Sviluppatore web*: in base alle specifiche ricevute dagli User Experience specialist, scrive e verifica il codice in HTML/Javascript, funge anche da designer grafico per i dettagli.
- *Tester*: Verifica moduli software scritti da altri, segue appositi percorsi di test e documenta l'esito delle prove.
- *Capo progetto*: progettista high-level, coordina il lavoro dei programmatori fissando le scadenze per le varie fasi e spesso tiene anche rapporti con il cliente.
- *Capo area*: figura presente nei progetti grandi, svolge le stesse funzioni del capo progetto in un'area ristretta.
- *Amministratore di sistema*: chiamato anche sistemista, è l'amministratore di server, applicativi, e rete. In sistemi grandi possono esserci diversi sistemisti, devono garantire il buon funzionamento costante di quanto a lui affidato e spesso tiene anche i rapporti con gli utilizzatori finali.
- *SRE*: Site Reliability Engineer è responsabile per la disponibilità, latenza, prestazione ed efficienza, gestione del cambiamento e risposta all'emergenza dei servizi assegnati (approccio di Google, Netflix ed altri).
- *Amministratore DB*: è l'amministratore del database server, deve garantire il buon funzionamento costante del DB con anche l'integrità dei dati.
- *Venditore*: controparte dell'acquirente, ha competenza economica, di mediazione e di relazione -> i migliori spesso sono di provenienza tecnica

Per quanto riguarda le *terze parti* abbiamo:

- *Consulente agli acquisti*
- *Solution Provider*

Per i ruoli dei progetti **ERP (Enterprise Resource Planning, capitolo 2)** abbiamo:

- *Progettista completo*: grande esperienza sia nell'analisi di processo che nell'uso dell'ERP, deve suddividere le aree funzionali dell'azienda in parti "mappabili" sui moduli che formulano l'ERP.

- *Analista di processo*: conosce bene uno o più processi e le funzioni svolte dal modulo che lo implementa, definisce nel dettaglio che variazioni devono essere fatte nei processi aziendali o che personalizzazioni devono essere introdotte nell'ERP
- *Programmatore*: usa un linguaggio proprietario per customizzare l'ERP, i cambiamenti possono essere semplici parametrizzazioni dell'ERP stesso.
- *Analista funzionale*: ha esperienza di analisi di processo, scrive le specifiche funzionali di dettaglio.

Dimensioni del progetto	Ruoli
Molto piccole	Nessuna suddivisione
Piccole	Acquirente dirigente programmatore e tester in una sola persona
Medie	Acquirente, capoprogetto, analista, integratore, programmatore e tester
Grandi	Acquirente, alta dirigenza, capoprogetto economico e tecnico, capogruppo, analista, integratore, programmatore, tester, documentatore, garante qualità
Molto grandi	Come sopra più altri (es. esperto di dominio applicativo)

Per i *ruoli nei contesti di esercizio* distinguiamo:

- L'*utente finale* del sistema
- L'*utente evoluto* del sistema
- L'*amministratore di rete*
- L'*amministratore di sistema*
- L'*amministratore di DB*
- L'*amministratore di informatica utente*: è un sistemista, si occupa delle postazioni utente e di scanner/stampanti/fax etc. segue anche le problematiche di applicativi utente come la suite office e spesso deve occuparsi anche dell'hardware.
- *Responsabile sistemi informatici (EDP Manager)*: coordina tutta l'attività del sistema informativo, è il responsabile aziendale di alcune funzioni -> CIO è la sua evoluzione (Chief Information Officer).

I sistemi informativi possono anche essere classificati in base alle loro *funzioni*, distinguendo le seguenti categorie di aziende:

- Manifatturiere
- Telecomunicazioni

- Banche ed assicurazioni
- Pubblica Amministrazione: per i comuni di medie dimensioni si tratta di servizio e gestione di sistemi, per i comuni grandi oltre al servizio e la gestione è presente anche uno sviluppo applicativi da software house a capitale pubblico. Per le province ci sono CED medio-grandi che si occupano di servizio e sviluppo interno, per le regioni lo sviluppo di grandi servizi avviene tramite software house connesse e consulenti esterni.
- Sanità

I nuovi profili standardizzati: European E-commerce Framework

Nuove leggi impongono la standardizzazione dei profili professionali nell'informatica, vengono definiti i criteri generali delle figure professionali operanti nei settori ICT. Alcune definizioni utili sono:

- *Conoscenze*: assimilazione di informazioni, relative ad un settore. Sono teoriche e pratiche
- *Abilità*: applicare le conoscenze e usare il know how necessario per portare a termine compiti e risolvere problemi; sono cognitive e pratiche.
- *Competenze*: comprovata capacità di usare conoscenze, abilità e capacità personali, sociali in situazioni di lavoro o di studio e nello sviluppo professionale e personale. Sono descritti in termini di responsabilità ed autonomia.

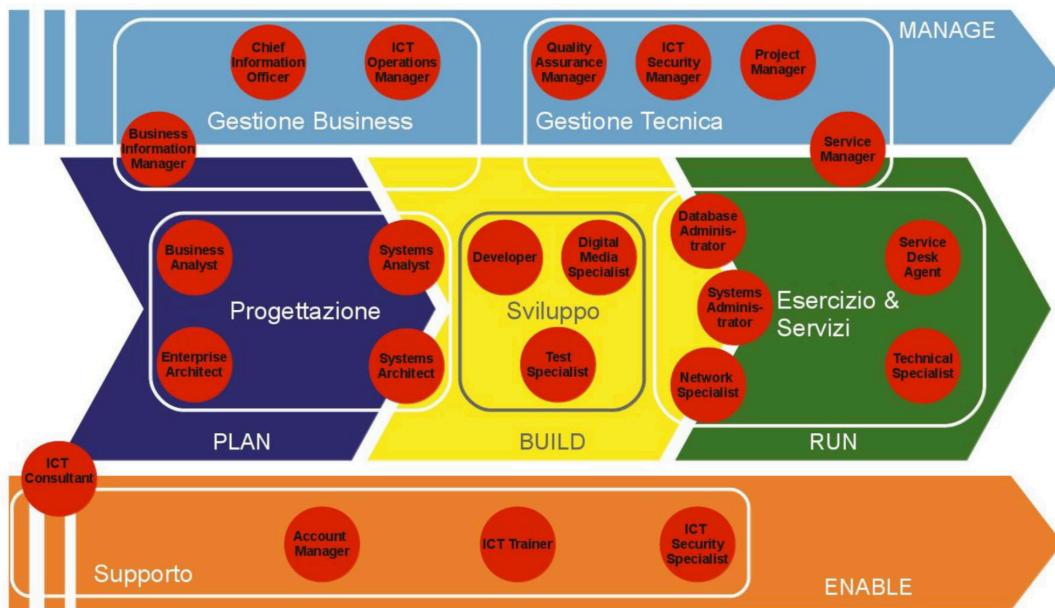
Ambiti standard per l'ICT:

- *Pianificazione strategica e progettazione (plan)*: allineamento strategie SI e di business, gestione dei livelli di servizio, sviluppo del business plan, pianificazione di prodotto
- *Sviluppo e implementazione (build)*: progettazione e sviluppo, integrazione di sistemi, testing, produzione della documentazione
- *Esercizio (run)*: supporto dell'utente, erogazione del servizio, supporto al cambiamento e gestione del problema
- *Supporto (enable)*: sviluppo della strategia della sicurezza informatica, sviluppo della strategia della qualità ICT, sviluppo dell'offerta, delle vendite, Istruzione e formazione etc.
- *Gestione (manage)*: formulazione delle previsioni, gestione del rischio, gestione delle relazioni, gestione del progetto e del portfolio, IT Governance etc.

Le macroaree standard per i profili sono:

- *Business management*: gestione lato business, i profili tipici sono *Chief Information Officer, Business Information Manager, ICT Operation Manager*
- *Technical Management*: gestione tecnico operativa, i profili tipici sono *quality assurance manager, ict security manager, project manager, service manager*

- *Design*: analisi e progettazione, si occupano del settore i *business analysts*, *systems analysts*, *enterprise architect*, *systems architect*.
- *Development*: ossia sviluppo, profili tipici: developer, digital media specialist, test specialist
- *Service e operation*: garanzia di esercizio, i ruoli tipici sono: database administrator, systems administrator, network specialist, technical specialist, service desk agent.
- *Support*: attività di supporto, i profili principali sono: ICT consultant, account manager, ICT trainer, ICT security specialist.



ESEMPIO AREA SISTEMI INFORMATIVI UNIPR

UOS = unità organizzativa di sede, UOC = unità operativa complessa

PLAN: *UOC pianificazione e gestione della domanda*, per l'allineamento strategie IS e di Business, gestione dei livelli di servizio, sviluppo business plan.

BUILD: *UOS Realizzazione Servizi*, per lo sviluppo di applicazione, integrazione dei componenti, produzione della documentazione etc.

RUN: *UOS Erogazione Servizi*, assicura l'erogazione di servizi informatici d'ateneo.
UOS supporto utenti per garantire l'assistenza agli utenti.

ENABLE: *UOC pianificazione e gestione della domanda*, per la gestione del contratto, l'identificazione dei fabbisogni e gli acquisti. *UOS Sicurezza, processi IT e servizi di collaborazione* per lo sviluppo della strategia per la sicurezza informatica

MANAGE: *UOC pianificazione e gestione della domanda*, per la gestione delle relazioni. *UOS Sicurezza, processi IT e servizi di collaborazione*. *UOS Sicurezza*,

processi IT e servizi di collaborazione per il miglioramento dei processi e la gestione del rischio e della sicurezza dell'informazione.

I profili professionali dell'IT: il modello EUCIP

EUCIP è il sistema europeo di riferimento per le competenze ed i profili professionali informatici. Il sistema di profili è articolato in 22 mestieri ICT che raggruppano tutte le principali figure professionali del mercato e ai quali associate delle certificazioni. Lo standard è basato su un dizionario di oltre 3000 unità elementari di conoscenze, articolate su un livello di base che comprende le conoscenze e competenze comuni ai profili professionali e su un livello specialistico che riguardano le conoscenze e competenze che caratterizzano i profili professionali e il profilo specialistico IT administrator.

Le unità elementari coprono le tre aree fondamentali del ciclo di vita dei sistemi ICT:
Area “Pianificazione” (Plan): orientata all’analisi dei requisiti in ambito ICT e alla pianificazione dell’utilizzo delle tecnologie stesse nell’ambito delle organizzazioni.
Area “realizzazione” (Build): Comprende i processi di specifica, sviluppo ed acquisizione di sistemi ICT.

Area “Esercizio” (Operate): Riguarda l’installazione, la supervisione e la manutenzione di sistemi informatici.

I 21 profili di livello elettivo si possono raggruppare in 7 gruppi professionali all’interno del settore IT:

1. *Business Innovation agent*: fanno parte di questo gruppo l’analista di sistemi informativi (identifica i requisiti per i sistemi ICT e nel definire modelli di flussi informativi), capoprogetto di sistemi informativi e analista business
2. *Solution Consultant*: consulente di logistica, consulente di soluzioni aziendali e consulente per la vendita.
3. *IT Business manager & professional*: responsabile commerciale, revisore di sistemi informativi, responsabile di sistemi informativi
4. *Technical Advisor*: progettista di sistemi informatici, progettista delle telecomunicazioni, consulente per la sicurezza
5. *Software Designers*: esperto di applicazioni web e multimediali, system integration e test engineer, analista programmatore.
6. *Operational manager*: responsabile di Basi di dati, responsabile di rete, data center and configuration manager.
7. *Service Support Specialist*: supervisore di un centro di assistenza, formatore IT, sistemista multipiattaforma

PLAN: 1-2-3, BUILD: 1-4-5-6 OPERATE: 4-6-7

Capitolo 9 – Introduzione alla sicurezza informatica

Gli obiettivi della sicurezza informatica -> **CIA (+2)**:

- **Confidenzialità**: le informazioni devono essere rese inaccessibili a terzi.
- **Integrità**: deve essere possibile verificare se le informazioni sono state modificate da terzi.
- **Disponibilità (Availability)**: il sistema informatico nel suo complesso deve continuare ad operare correttamente.
- **Autenticazione**: deve essere possibile verificare che un utente è davvero colui che afferma di essere e che un documento digitale è davvero stato creato da un certo utente
- **Non ripudio**: non deve essere possibile poter disconoscere le informazioni che si è generato

La prima normativa è stata menata nel **1996**, la legge sulla protezione dei dati personali prevedeva l'obbligo di adozione delle misure *minime* di sicurezza e delle misure *idonee*. Nel **2003 d.lgs. 196/03** “codice in maniera di protezione dei dati personali” -> autenticazione informatica, adozione di procedure di gestione delle credenziali di autentificazione, protezione degli strumenti elettronici e dei dati rispetto ai trattamenti illeciti, ad accessi non consentiti e a determinati programmi informatici. Inoltre, vengono citate la tenuta di un documento aggiornato programmatico sulla sicurezza e l'adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi. Nel **2018 UE GDPR (general data protection regulation)**, impostazione sistemica e si passa da una logica di *minimo* ad una logica di *adeguato*: muta l'approccio da formale in sostanziale e proattivo, consolida le garanzie ed i diritti dell'interessato per il controllo delle proprie informazioni ed inoltre accresce le responsabilità del titolare e del responsabile dei dati. Le *figure previste* da questa legge sono:

- *Titolare del trattamento*: indicati gli oneri connessi alla titolarità, le misure idonee in relazione ai trattamenti, l'autonoma valutazione dei rischi.
- *Responsabile del trattamento*: accountability diretta del responsabile anche in ordine al risarcimento del denaro, contratto per regolare i rapporti con il titolare ed infine possibile impiego di sub-fornitore con delega del titolare.
- *Data Protection Officer* (non prevista nella direttiva europea del '95): obbligatorio per la PA, “suggerito” per gli altri titolari in quanto figura che svolge un ruolo di “cerniera” nei confronti delle Autorità.

Per quanto riguarda dell'accesso ai dati si parla di:

- Consenso: consenso di forme implicite nella direttiva del '95, necessario che vi sia una forma esplicita ed inequivocabile
- Notificazione: obbligo per direttiva '95, nessun obbligo per il GDPR

- Tipologie dei dati: per il '95 dati personali, sensibili e giudiziari. Per il GDPR i dati sensibili diventano particolari e viene introdotta la definizione dei dati genetici, biometrici e pseudo-anonimi.
- Diritti dell'interessato: nella direttiva europea del '95 si parla di conferma del trattamento, rettifica, cancellazione e limitazione per determinate operazioni di trattamento mentre nel GDPR si parla di diritto all'oblio (cancellazione dagli archivi online, anche a distanza di anni, di tutto il materiale che può risultare sconveniente e dannoso per soggetti che sono stati protagonisti in passato di fatti di cronaca) e diritto alla portabilità dei dati.

La sicurezza può essere vista come processo che comprende diverse fasi:

1. *Business impact analysis*, ovvero l'analisi dei rischi e dei possibili danni
2. *Security Policy*, l'insieme di regole, principi e procedure che stabiliscono il modo con cui l'azienda gestisce protegge e controlla le proprie risorse informatiche e le informazioni
3. *Security Plan*: implementazione delle regole del security policy
4. *Disaster Recovery Plan*: organizzazione del piano di recupero delle informazioni in caso di "disastri" (attacchi informatici e non solo...)
5. *Security Audits*: verifiche sull'efficacia del sistema di sicurezza

L'**ISO 27001:2013** descrive un processo con *sei fasi*:

1. Definire una politica della sicurezza
2. Definire un ambito per il sistema di gestione della sicurezza dell'informazione (*ISMS*)
3. Eseguire una valutazione del rischio della sicurezza
4. Gestire il rischio identificato: Risk Treatment Plan (*RTP*)
5. Scegliere i controlli da realizzare ed applicare
6. Preparare una *dichiarazione di applicabilità*, deve riportare i controlli selezionati come necessari e la relativa giustificazione per l'inclusione.

L'**ISO 27002:2013** descrive i controlli che possono realizzare un *ISMS*

CLUSIT è l'associazione Italiana per la sicurezza informatica (senza fini di lucro), nel 2017 parlava di anno peggiore di sempre in termini di evoluzione delle minacce cyber, da un punto di vista qualitativo e quantitativo -> maggiore superficie d'attacco per diffusione di device IoT e dello smart working, si parla di allarme rosso. Nel 2021 -> si parla di far west digitale con 6 trilioni di perdite.

Con Governo Draghi nasce *l'agenzia per la cybersicurezza nazionale ACN*, la cyber-intelligence però resta ai servizi segreti.

Gli attacchi informatici possono essere rischi diretti o indiretti per l'azienda: per le *perdite indirette* si riferisce ai potenziali clienti, impatto negativo sul proprio brand o perdita di vantaggi sui propri prodotti. I rischi diretti sono furti di informazioni,

denaro o dati sui clienti o perdita di produttività dovuta a corruzione dei dati e a spese e tempo per il ripristino.

Business Continuity e Disaster Recovery

In un contesto di sicurezza informatica è opportuno trattare anche le problematiche legate ad eventi accidentali, esistono leggi che regolamentano la protezione dei dati dalle perdite accidentali. Talvolta queste tecniche sono un'ottima risposta anche a problemi legati ad azioni fraudolente umane.

La **business impact analysis** risponde alle seguenti domande (tramite questionari, interviste o incontri con il personale chiave dell'IT): quali processi aziendali hanno un'importanza strategica, quali disastri potrebbero accadere, quale impatto avrebbero sull'organizzazione da vari punti di vista (finanziario, legale, vitale, sulla reputazione etc.), e qual è il periodo temporale per poter recuperare l'operatività. Una possibile classificazione dei danni degli eventi può essere data da:

- *Danni trascurabili* ovvero nessun costo o danno significativo
- *Danni minori* un evento non trascurabile ma senza un impatto materiale sul business.
- *Danni maggiori* impatta uno o più dipartimenti e può impattare anche i clienti esterni.
- *Crisi* ha un impatto materiale o finanziario determinante sul business-

L'*interruption window* è l'intervallo temporale in cui l'azienda può attendere tra l'evento e una ripresa del servizio, il *SDO (Service Delivery Objective)* è il livello di servizio in alternate mode ed il *Maximum Tolerable Outage* è il tempo massimo tollerabile in Alternate Mode.

La **Business Continuity** è la capacità di offrire servizi critici in caso di interruzione forzata da eventi avversi.

Il *disaster recovery* è l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare i sistemi, dati e le infrastrutture necessarie all'erogazione di servizi di business. L'*alternate process mode* è il servizio offerto dal sistema di emergenza/backup. Il *disaster recovery plan (DRP)* indica come transitare in alternate process mode, mentre il *restoration plan* come ritornare al modo normale di sistema. L'**ISO 22301** copre aspetti di sicurezza del BCM (Business Continuity Management), è basato su un ciclo PDCA. Un sistema per BCM dovrà contenere la documentazione per:

1. Obiettivi del BCMS
2. Business Continuity policies
3. Descrizione dei ruoli e delle responsabilità
4. Risk assessment e Business Impact Analysis (BIA) report
5. Business continuity plan
6. Comunicazione, addestramento ed un piano del rischio
7. Esercizi e procedure di prova

8. Valutazioni, management review e procedure di verifica dell'efficacia del sistema

9. Azioni preventive e correttive

La *classificazione dei servizi* suddivide i servizi in:

- *Servizio critico*: non può essere effettuato manualmente e la tolleranza all'interruzione è molto bassa
- *Servizio vitale*: può essere eseguito manualmente solo per un periodo di tempo molto limitato
- *Servizio sensibile*: può essere eseguito manualmente per un periodo di tempo, ma può costare di più per il personale.
- *Servizio non sensibile*: può essere eseguito manualmente per un periodo di tempo anche esteso con pochi costi addizionali ed uno sforzo minimo di recupero.

RPO - Recovery Point Objective: quanto tempo all'indietro può essere recuperato, "fino a quanto all'indietro si può fallire", Backup images per un RPO lungo mentre per un RPO breve si usano i dischi RAID.

RTOP - Recovery Time Objective: quanto tempo si può operare senza il sistema.

Gli *orphan data* sono dati che sono persi e mai recuperati.

La *replica dei dati (BACKUP)* può avvenire tra il sistema di storage locale ed uno remoto, esistono due modalità principali: la **replica sincrona** che garantisce perdite nulle per mezzo di write sincrone, il limite è la distanza geografica (35-100km) per garantire una latenza molto bassa. La **replica asincrona** è completata quando confermata dallo storage locale, il remoto è aggiornato con un certo ritardo, in caso di crash locale il sistema remoto potrebbe non essere aggiornato.

Per la conservazione dei dati è necessario centralizzare la raccolta dei file almeno su server dipartimentali, un backup automatico dei dischi dei client diventa ingestibile, gli utenti devono procedere alla salvaguardia dei propri dati.

Per un'operazione di backup bisogna decidere se utilizzare un approccio *incrementale* o *alle differenze* (backup incrementale esegue copie dei dati modificati dall'ultimo backup mentre il backup differenziale esegue copie dei dati modificati dall'ultimo backup completo) ed una *politica di salvataggio* (ogni quanto tempo fare un backup dei dati).

La fase di installazione e configurazione di un sistema assorbe molto tempo, per questo motivo si introduce il *backup dell'immagine*: in funzione dello scopo del sistema si definiscono tutti i componenti software della dotazione base e con un programma (es. Norton Ghost o DiskImage) si crea un'immagine dell'installazione che in caso di problemi viene utilizzata per ripristinare la configurazione base.

Le minacce umane sulla sicurezza

I principali tipi di attacco sono:

- *Intrusione*: accedere a dati riservati, entrando in un database o in un archivio di posta e/o documenti, in un filesystem, in un directory service, impadronirsi di indirizzi di posta o di un archivio di chiavi e/o password.
- *Impersonificazione*: assumere un'identità, entrare in un sistema con privilegi non propri, potere usare a scrocco servizi non propri, accedere a risorse finanziarie non proprie etc.
- *Intercettazione*: effettuare transazioni finanziarie fraudolente, rubando codici di carte di credito, codici di accesso home banking oppure attaccando direttamente sistemi bancari.
- *Abuso*: usare risorse senza averne diritto, per esempio accedendo ad una rete esterna, uso di servizi in modo contrario alle regole, o spamming.
- *Denial-of-Service*: mandare fuori servizio un sistema, bloccando un servizio o un server, la rete o il DNS.

Esistono diversi tipi di attaccanti, i principali sono gli hacker, i cracker, le spie industriali, sabotatori, impersonale, virus.

Le principali vulnerabilità dei sistemi sono: vulnerabilità dei dati, dei programmi applicativi, dei programmi server, dei sistemi operativi, dei sistemi fisici e delle trasmissioni.

Con *intrusione in un sistema* si intende l'accesso non autorizzato ad un servizio disponibile in un server, mediante la connessione di terminale remoto oppure tramite ingresso sul disco.

Da un punto di vista tecnico possono esserci degli:

- *Attacchi alle password*: mediante l'utilizzo di dizionari, tentativi successivi, numero massimo di tentativi o perfino tentativo di cattura dei file delle password
- *Attacchi alle reti*: intercettazione dei dati intransito, packet sniffing, analisi di quanto intercettato, attacco ad un nodo, footprinting
- *Attacchi alla posta elettronica*: overflow (inviare messaggi voluminosi per saturare capacità delle caselle di posta), spamming (invio di posta non autorizzata da un server di posta attaccato), mail impersonificate
- *Attacchi ai server Web*: il server web usa una parte del filesystem del computer server per le informazioni che mette a disposizione, gli attacchi tendono ad accedere all'esterno di tale "area riservata".
- *Crack delle password*: si può effettuare intercettando il traffico di rete utilizzando specifici programmi oppure utilizzando comandi net
- *Diventare Administrator* utilizzando utility di crack per agire sui file ed installare qualcosa nel sistema
- *Intercettazione dei tasti*: programmi che consentono di registrare tutto ciò che viene digitato sulla tastiera, consentendo di disporre di tutte le informazioni possibili.

Un **virus** è un insieme di istruzioni comprensibili dal computer che svolgono un'attività dannosa e/o fraudolenta, si mimetizza entro programmi o documenti che ne risultano infettati, i principali sono i *Virus degli eseguibili*: la versione più antica di virus, sostituiscono il proprio codice a parte del codice del programma, quasi sempre non aumentano la dimensione o modificano la data del programma infettato. Altri virus sono il virus del BIOS, del terminale, dei boot sector, Web Virus, Virus misti.

La gestione della sicurezza

I punti chiave della gestione della sicurezza sono: le tipologie di applicativi in uso, l'esperienza tecnica e pratica degli amministratori e degli utenti, la politica del rischio stabilita in azienda ed il rapporto costi/benefici, tra le misure di sicurezza adottate ed il loro costo. Bisogna tenere in mente che non esiste una politica buona per tutti, deve essere decisa caso per caso considerando anche i fattori elencati in precedenza.

L'*approccio militare* consiste nel garantire sicurezza assoluta scoprendo in anticipo i tipi di attacco e prevenirli anche grazie all'aiuto della tecnologia, in questo caso però la sicurezza assorbe troppe risorse e diviene un ostacolo per il Business.

L'*approccio risk management* vede la sicurezza come fattore relativo, ci sono molti rischi e bisogna tenerli in considerazione; bisogna tenere in considerazione anche le molteplici soluzioni che dipendono dal contesto. Questo approccio prevede l'accettare il rischio e ridurlo con l'utilizzo della tecnologia e di procedure opportune e quando è possibile trasferendolo (mediante outsourcing e/o assicurazioni).

Una conoscenza d'insieme del sistema è indispensabile per pianificare qualsiasi politica di sicurezza, le misure di sicurezza non devono mai essere di ostacolo reale al funzionamento dei programmi: bisogna cercare il giusto compromesso fra sicurezza ed uso.

Il punto debole della sicurezza sono molto spesso gli *utenti*, qualsiasi operazione di sicurezza che richieda un intervento esplicito dell'utente o che richieda uno sforzo di attenzione è statisticamente destinato a fallire.

Nella pratica una PMI (piccola media impresa) dovrebbe avere un po' di buon senso: antivirus e firewall aggiornati, filtri sui router, auditing, controllo accessi interni, creare una lista di applicazioni considerate affidabile ed impedendo l'installazione di qualsiasi altra applicazione, configurando in maniera sicuro l'hardware ed il software, limitare il più possibile gli utenti con i privilegi di amministratori/root sia a livello locale che di dominio, configurare gli account degli utenti affinché abbiano i privilegi minimi richiesti per eseguire le attività loro assegnate, impostare una politica di autenticazioni attraverso password complesse, predisporre un'efficace difesa del perimetro della rete aziendale attraverso strumenti informatici.

La gestione delle *password* è una delle attività più complesse, occorre forzare gli utenti all'aggiornamento periodico delle password (alternanza maiuscola-minuscola,

numeri e altri caratteri e di lunghezza minima). Gli addetti ai sistemi informatici devono rendere il management consapevole dei rischi.

Un altro fattore importante per garantire maggiore sicurezza ad un'azienda è l'aggiornamento periodico dei sistemi, verificando periodicamente dei bollettini di sicurezza. Spesso una patch di sicurezza corregge dei problemi ma ne crea degli altri; tuttavia, se il problema è critico è necessario comunque applicare la patch il prima possibile. Per contrastare i virus è necessario implementare gli antivirus, che devono funzionare in automatico sui nuovi file, deve esistere una combinazione fra server e client. APPROFONDIMENTO: uso dell'IA da parte delle piccole/medie aziende contro gli attacchi online.

L'ISO 27000 e la legislazione

Lo standard UNI CEI ISO/UEC 27001:2006 è la norma internazionale di riferimento che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni, include aspetti relativi alla sicurezza logica, fisica ed organizzativa. È composta da 6 sezioni:

1. **ISO 27001**: fornire un modello per stabilire, attuare, rendere operativo, il monitoraggio, la revisione, il mantenimento e il miglioramento di un Security Management Information System.
2. **ISO 27002** codice di condotta per la sicurezza informatica, delinea centinaia di potenziali controlli e meccanismi di controllo.
3. **ISO 27003** fornisce un aiuto e guida per implementare un ISMS (information security management system).
4. **ISO 27004** fornisce le linee guida per lo sviluppo e l'uso di misure per la valutazione dell'efficacia di un sistema di gestione implementando la sicurezza delle informazioni e controlli.
5. **ISO 27005** copre la gestione del rischio nell'information security
6. **ISO 27006** standard che offre le linee guida per l'accreditamento di organizzazioni che offrono la certificazione

L'**ISO 27017** fornisce una guida per servizi cloud basata su 37 controlli derivanti dalla ISO 27002 e su sette controlli aggiuntivi (suddivisione delle responsabilità tra fornitore e clienti dei servizi cloud, rimozione delle attività alla cessazione di un contratto, configurazione della virtual machine, protezione e separazione degli ambienti virtuali dei diversi clienti, allineamento degli ambienti virtuale e cloud, monitoraggio attività del cliente all'interno dell'ambiente cloud e attività amministrative e procedure connesse con l'ambiente cloud).

L'**ISO 27018** stabilisce le linee guida per l'implementazione di misure di protezione delle *informazioni di identificazioni del personale (PII)*. I responsabili del trattamento

delle PII possono essere soggetti a leggi, regolamenti e obblighi aggiuntivi, che non si applicano ai responsabili del trattamento delle PII.

Alcune definizioni legali importanti sono:

Sistemi informatici: qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnessi o collegati, uno o più dei quali in base ad un programma eseguono l'elaborazione automatica dei dati.

Dati informatici: qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico.

Attacco ad un dato: per copiarlo o modificarlo senza autorizzazione, che non impedisce l'ulteriore funzionamento del sistema informatico che lo ospita

Attaccato ad un sistema: per impedire il suo uso e l'accesso a tutti i dati in esso memorizzati.

A livello Europeo le leggi più importanti sono GDPR -> regolamento generale sulla protezione dei dati e la convenzione di Budapest

In Italia la ratifica della convenzione e l'articolo 24 bis del DL 231 e articoli 615 e seguenti del Codice penale.

Cenni alla sicurezza per i sistemi di controllo industriali OT

Gli attacchi agli ICS sono in aumento e spesso sono condotti in maniera molto specifica con una conoscenza approfondita del target, il rischio può essere molto alto per i sistemi di controllo di infrastrutture critiche o di impianti industriali essenziali.

Spesso la rete industriale è connessa alla rete aziendale, quindi attaccabile, inoltre alcuni attacchi vengono svolti mediante mezzi fisici (es. chiavetta USB). L'isolamento del sistema industriale è sempre più un'illusione con la presenza di upload al SI/Cloud, aggiornamenti dal sito del produttore e manutenzioni da remoto.

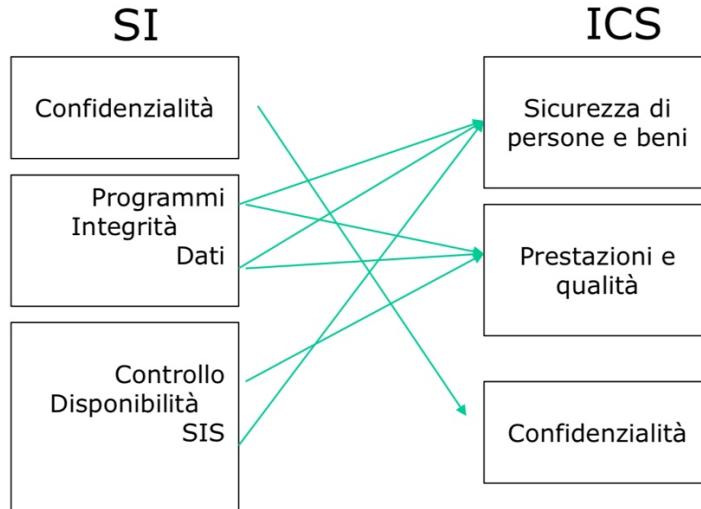
L'impatto di un attacco ai sistemi industriali può essere molto alto per interruzioni prolungate della produzione, per riduzione della qualità dei prodotti o perfino il danneggiamento delle macchine.

I tipi di attacco più comuni sono: Ransomware, server access, DDoS, Credential harvesting.

La **resilienza** di un SI è la sua capacità di continuare a funzionare mentre è sotto attacco, è una misura di quanto un'organizzazione possa gestire un attacco informatico o una violazione dei dati. I 4 elementi della cyber resilienza sono:

- *Gestire e proteggere:* essere in grado di identificare, valutare e gestire i rischi associati alla rete ed ai sistemi informativi
- *Identificare e rilevare:* monitoraggio continuo della rete e dei sistemi informatici per rilevare anomalie e potenziali incidenti di sicurezza informatica
- *Rispondere e recuperare:* l'implementazione di un programma di gestione della risposta agli incidenti garantisce la continuità del business.

- *Governare e assicurare*: assicurarsi che il programma sia supervisionato dai vertici dell’organizzazione e inserito nel business “as usual”, nel corso del tempo dovrebbe allinearsi sempre più strettamente con gli obiettivi aziendali più ampi.



Le principali differenze tra IT (information technology) ed OT (operational technology) riguardano quattro aspetti:

1. Le funzionalità previste e le relative necessità: sistema IT non real-time a differenza dell’OT. Il reboot non è accettabile come risposta ad un attacco per i sistemi OT (lo è per i sistemi IT).
2. La tecnologia utilizzata: i sistemi OT possono non avere abbastanza memoria e risorse di calcolo per supportare l’aggiunta di capacità e sicurezza, molti protocolli di comunicazioni sono proprietari e standard.
3. Il ciclo di vita del sistema: 3-5 anni per un sistema IT, 15-20 per un sistema OT
4. La gestione della sicurezza: Integrità dei dati e ritardo delle operazioni sono i rischi più importanti per un sistema IT. Per un sistema OT la sicurezza umana è fondamentale, seguita dalla protezione del processo, inoltre la tolleranza ai guasti è essenziale (anche un fermo momentaneo potrebbe essere inaccettabile)

Organizzazione e fattori umani	<i>Responsabilità, politiche, formazione</i>
Perimetro del cyberspazio e fisico	<i>Firewall, IDS, honeypots, controllo d’accesso fisico, protezione eventi avversi</i>
Rete	<i>Difesa contro sniffing, furti sessione o iden</i>
Endpoint (computer e dispositivi)	<i>Difesa dei SO e delle porte fisiche,</i>
Applicazioni	<i>Autenticazione, autorizzazione e auditing, vulnerabilità</i>
Asset mission-critical (dati o processi fisici)	<i>Sicurezza delle informazioni in memoria e nello storage</i>

Differenti livelli della sicurezza IT